JetBox 5630

Web User Manual

www.korenix.com

0.0.1

Copyright Notice

Copyright© 2013 Korenix Technology Co., Ltd.
All rights reserved.
Reproduction without permission is prohibited.

Information provided in this manual is intended to be accurate and reliable. However, the original manufacturer assumes no responsibility for its use, or for any infringements upon the rights of third parties that may result from its use.
The material in this document is for product information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Korenix assumes no liabilities resulting from errors or omissions in this document, or from the use of the information contained herein.
Korenix reserves the right to make changes in the product design without notice to its users.

Acknowledgments

Korenix is a registered trademark of Korenix Technology Co., Ltd.
All other trademarks or registered marks in the manual belong to their respective manufacturers.

Table of Content

Copyright Notice 2
Acknowledgments 2
Table of Content 3
Chapter 1 Getting Start 5
1-1 Web Server 5
1-2 Preparation for Web Interface 6
1-3 System Login 6
Chapter 2 System 7
2-1 Overview 7
2-2 Password 7
2-3 Scheduled Task 8
2-4 Startup 9
2-5 General Settings 9
2-6 Backup Configuration 10
2-7 Firmware Upgrade 11
2-8 Reboot 12
Chapter 3 Network 12
3-1 Status 12
3-2 Settings 13
3-3 WiFi Settings 13
3-4 3G Settings 16
3-5 Network Redundancy 18
3-6 Diagnostics 20
Chapter 4 Switch 21
4-1 Port Status 21
4-2 Port Control 21
4-3 VLAN 22
4-4 PVID 22
4-5 QoS 23
4-6 Rate Limit 26
Chapter 5 Routing 27
5-1 Status 27
5-2 Static Routes 28
5-3 OSPF 29
5-4 RIP 31
Chapter 6 Firewall 33
6-1 Forwarding 33

6-2 NAT 34
6-3 Filter 37
Chapter 7 VPN 39
7-1 OpenVPN 39
7-2 IPSec 42
7-3 Certificates 45
7-4 PPTP 46
7-5 L2TP 49
7-6 L2TPv3 52
7-7 CHAP-Secrets 54
Chapter 8 Serial 55
8-1 Port Settings 55
8-2 Serial to Network 55
8-3 ModBus Gateway 56

Chapter 1 Getting Start

1-1 Web Server

In JetBox5630, we will start web server automatically. You can see it with '**ps**' command.

```
1175 root     /lib/udev/udevd
1440 root     {hostenv.sh} /bin/sh ./hostenv.sh host /usr/lib/lua /usr/lib/lua
1448 root     lua /web/lucid.lua
```

The default path is /web/.

```
/web $ df
Filesystem                Size      Used Available Use% Mounted on
ubi0:rootfs              95.3M     34.6M     60.7M  36% /
ubi1:etc                  6.5M    580.0K      5.9M   9% /etc
ubi2:web                  6.5M      3.2M      3.3M  49% /web
ubi3:opt                104.4M      1.0M    103.3M   1% /opt
tmpfs                    30.0M     92.0K     29.9M   0% /tmp
tmpfs                   100.0M         0    100.0M   0% /home
tmpfs                     5.0M      4.0K      5.0M   0% /root
tmpfs                     1.0M         0      1.0M   0% /usr/etc
tmpfs                     1.0M         0      1.0M   0% /media
```

```
~ $ cd /web/
/web $
/web $ ls
build       host        hostenv.sh  lucid.lua   setup.lua
/web $
/web $
```

The default port number of web server is **80**.

NOTE

- If unnecessary, don't modify or delete any content in /web.
- We will keep the latest version and provide firmware to upgrade web server.

1-2 Preparation for Web Interface

Korenix web management page is developed by LUA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, Chrome, or Mozila, to configure the JetBox from anywhere on the network.

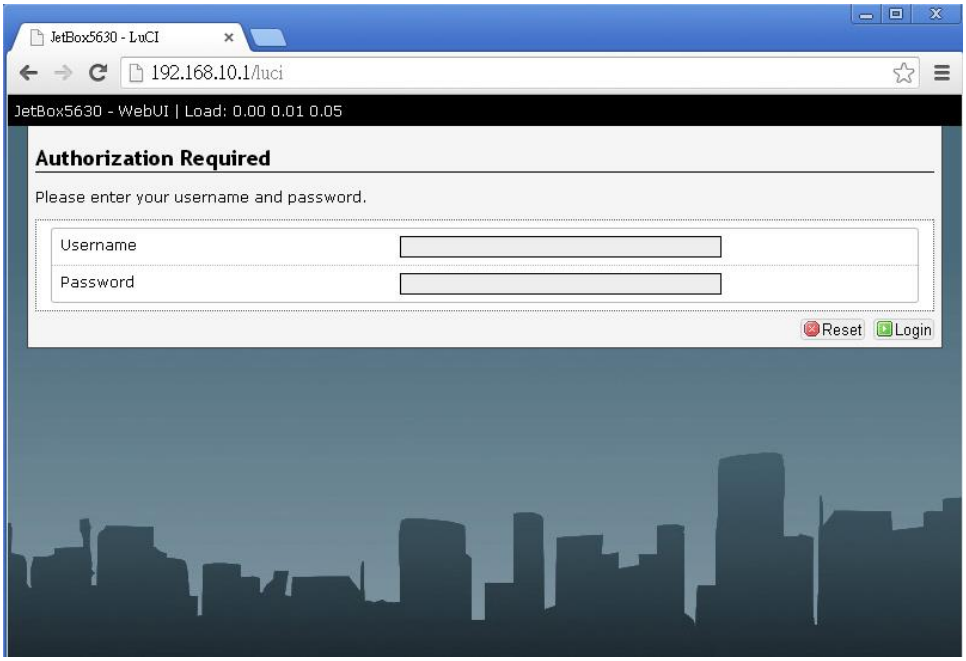
Before you attempt to use the embedded web interface to manage JetBox configuration, verify that your JetBox 5630 Series is properly installed on your network and that every PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
2. Wire DC power to the JetBox and connect it to your computer via LAN port.
3. Make sure that the LAN's default IP address is 192.168.10.1.
4. Change your computer IP address to 192.168.10.2 or other IP address which is located in the 192.168.10.x (Network Mask: 255.255.255.0) subnet.
5. Switch to DOS command mode in your computer and ping 192.168.10.1 to verify a normal response time.

1-3 System Login

Launch the web browser and Login.

1. Launch the web browser (Internet Explorer or Chrome) on the PC.
2. Type http://192.168.10.1 (or the IP address of the switch). And then press Enter.
3. The login screen will appear next.

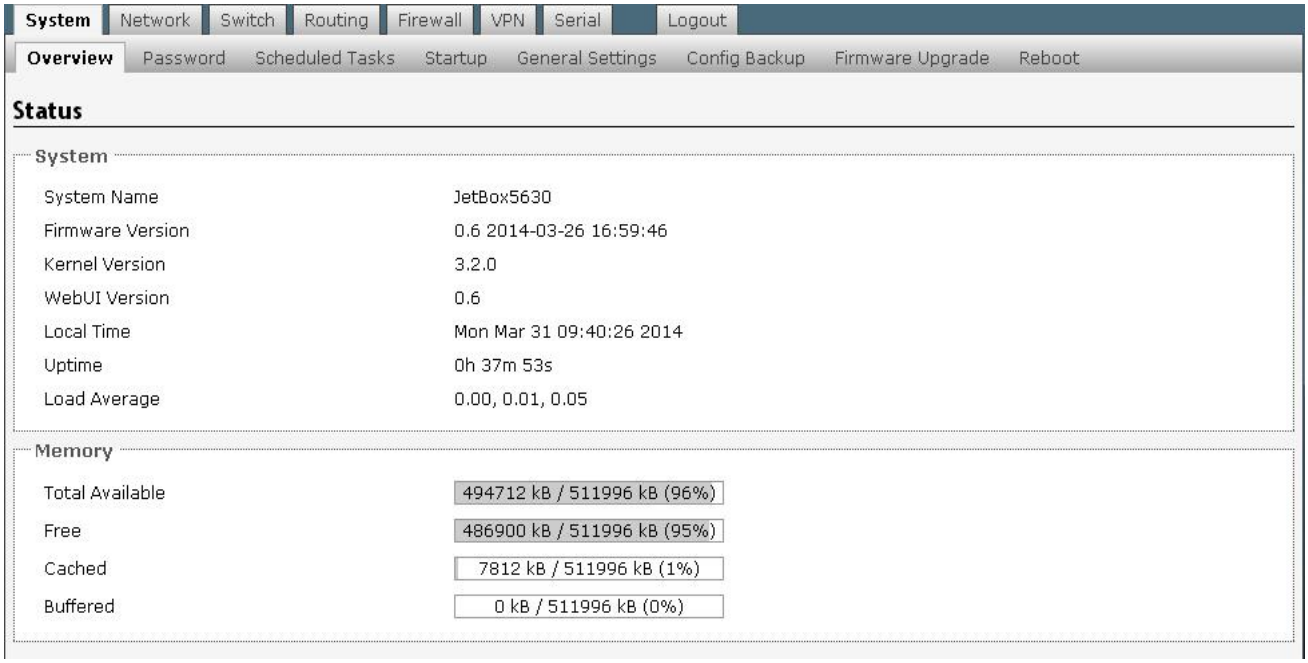


The default login user is **root** without password.

Chapter 2 System

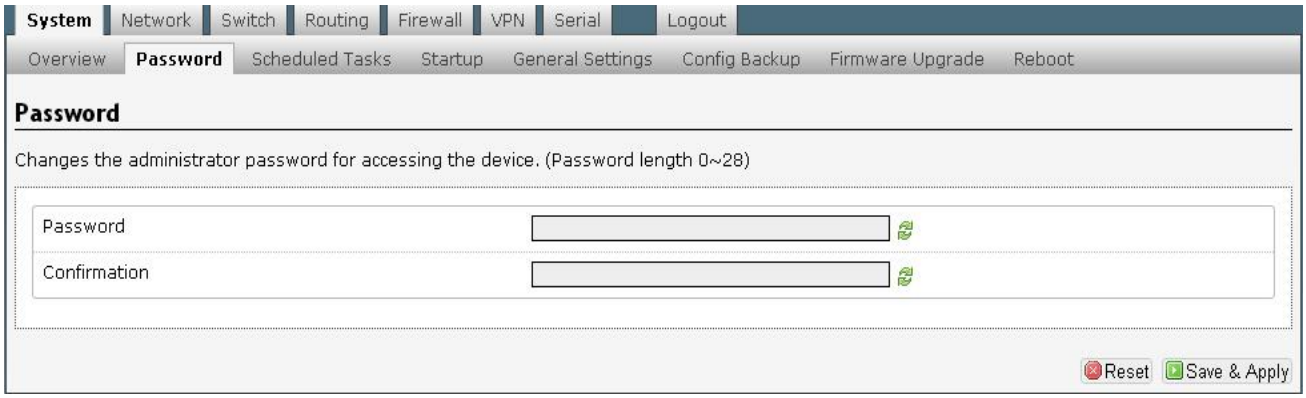
2-1 Overview

You can see system information on this section. Such as Hostname、Firmware version、WebUI version etc… and also display memory information.



2-2 Password

Change login password .



Password length : **0~28**

NOTE

- When you change web login password, it will also change system login password simultaneously

2-3 Scheduled Task

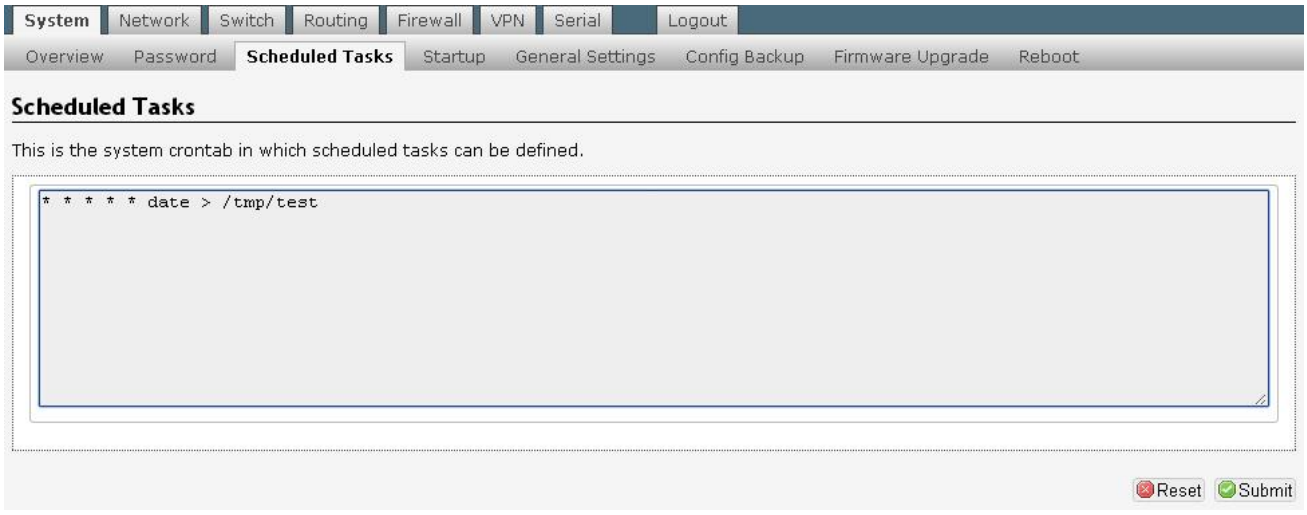
It is the same with Cron daemon.

Syntax :

A crontab file has five fields for specifying day, date and time followed by the command to be run at that interval.

```
*     *     *   *    *        command to be executed
-     -     -   -    -
|     |     |   |    |
|     |     |   |    +----- day of week (0 - 6) (Sunday=0)
|     |     |   +------- month (1 - 12)
|     |     +--------- day of month (1 - 31)
|     +------------ hour (0 - 23)
+-------------- min (0 - 59)
```

Example :

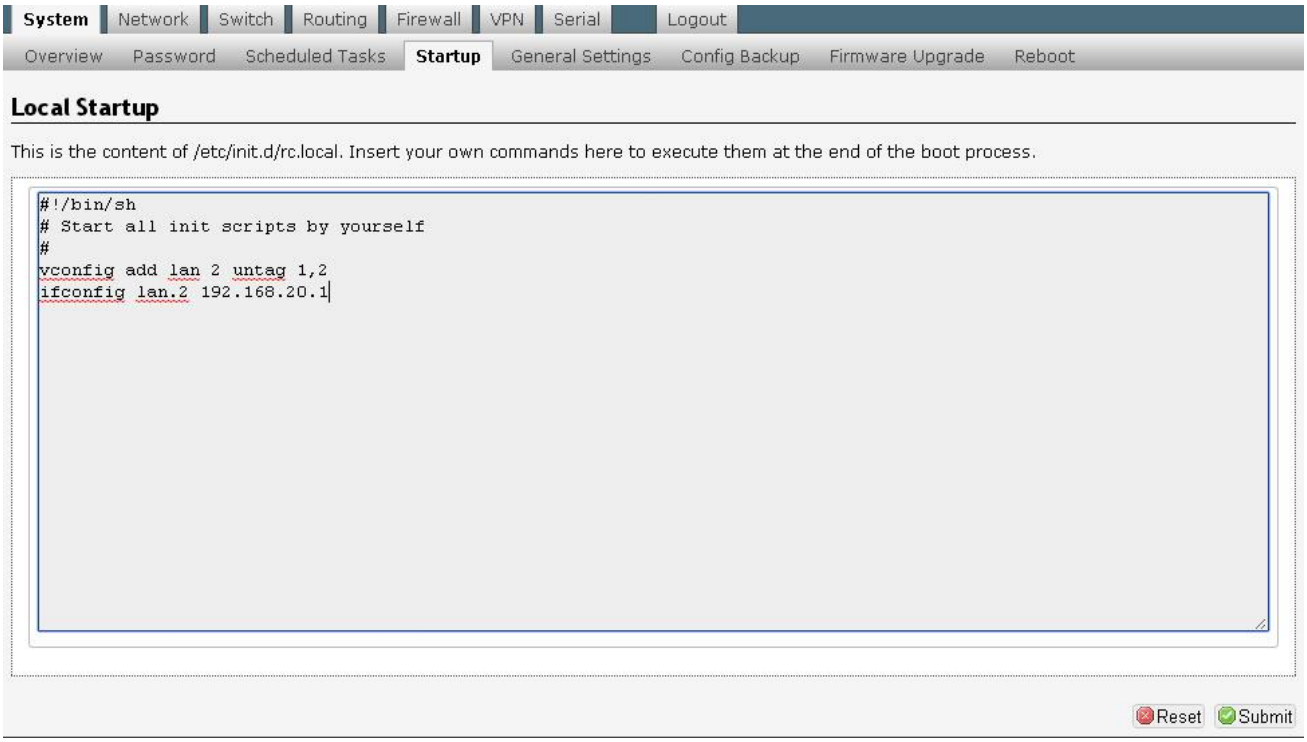


2-4 Startup

We provide a Startup script (**rc.local**) for user can run their program when system boot up.

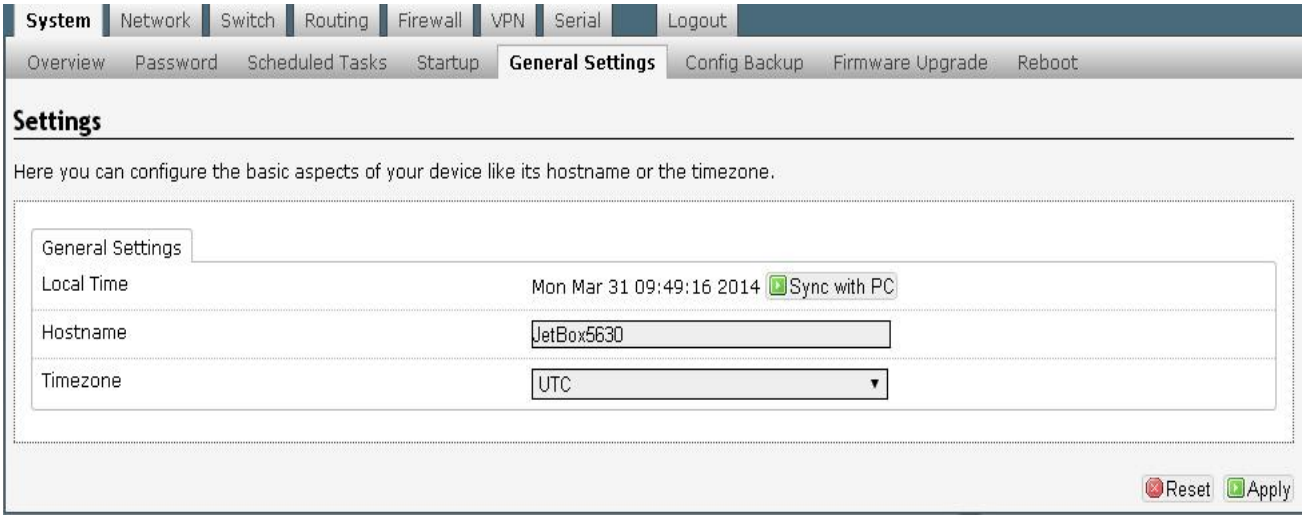
For example :

If we want to add a vlan 2 and set ip address 192.168.20.1 when system boot up, we can write these commands here. It will run automatically at the end of boot process.



2-5 General Settings

Here you can configure the basic aspects of your device like its Hostname or the Timezone.



Sync with PC :

It will get the UTC time from your PC. And local time have to be added with Timezone.

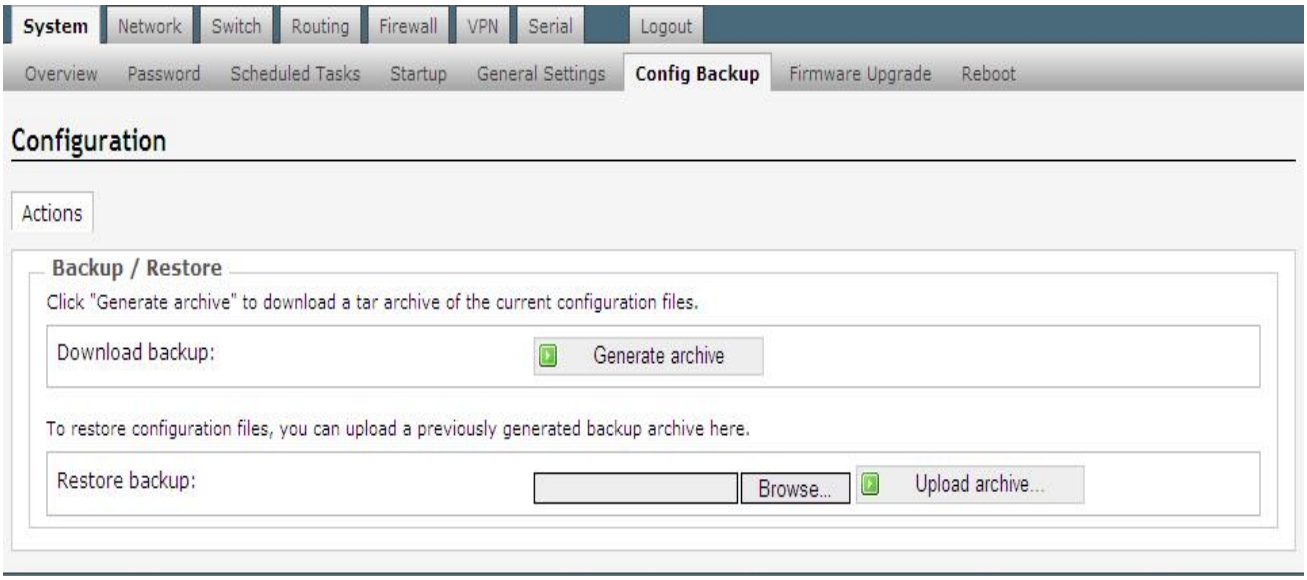
For example :

The UTC time of PC is **12:00:00 2013** and Timezone is Asia/Taipei.

So the local time will be **18:00:00 2013**.

2-6 Backup Configuration

In **Config Backup** page, user can use it to backup system configuration. It will backup all files in /etc. And user can apply these configurations to other JetBox.



Download Backup :

Click "Generate archive" to download a tar archive of the current configuration files

Restore Backup :

Upload a previously generated backup archive to restore configuration files.

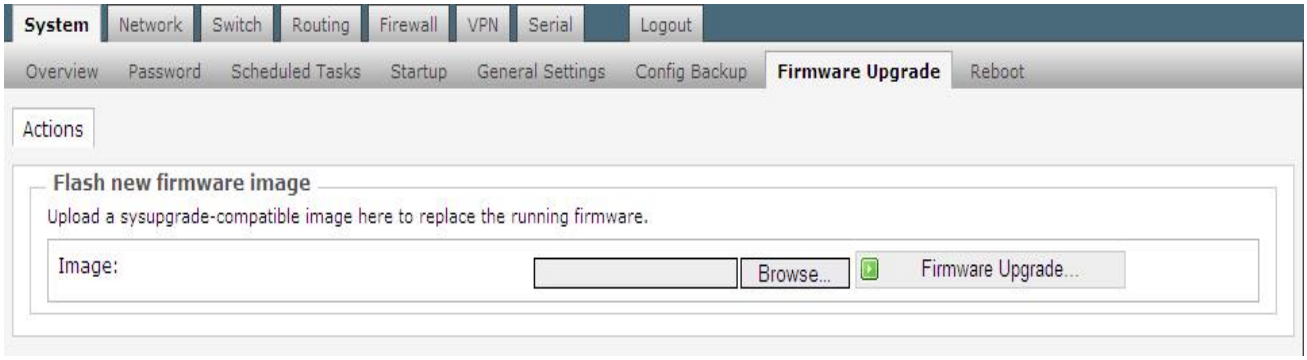
NOTE

- Restore configuration only extract all configuration files to /etc. It will not delete any files in /etc.

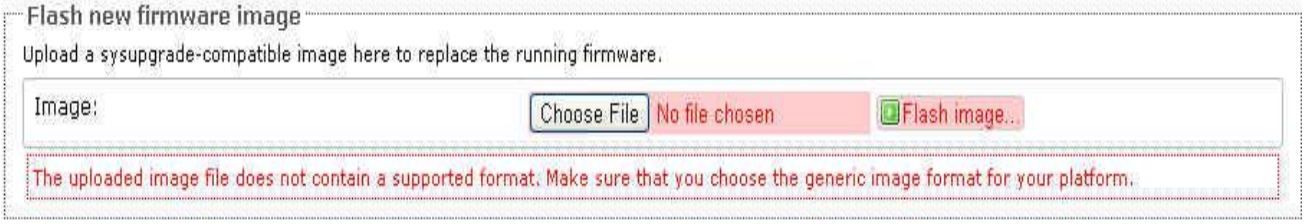
2-7 Firmware Upgrade

It is the same as firmware_up command in JetBox. User can upgrade firmware via Web or JetBox console.

Flash image :

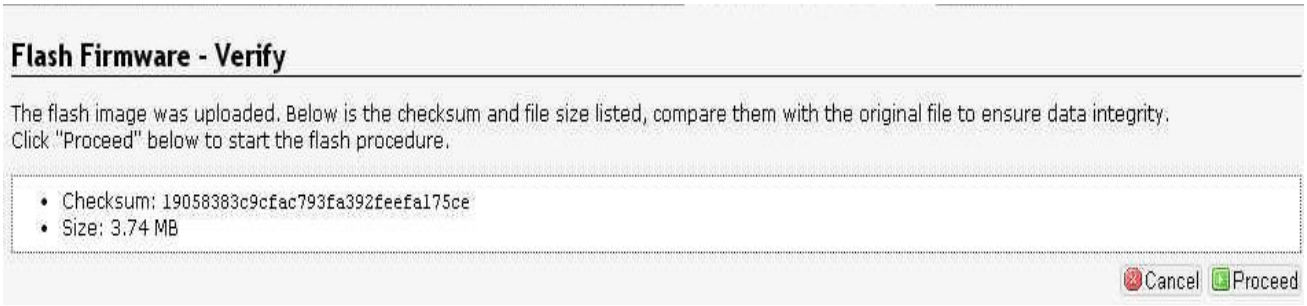


After select the image file, click it to start firmware upgrade. It will verify the image is valid or not.


Flash new firmware image
Upload a sysupgrade-compatible image here to replace the running firmware.
Image:
Choose File
No file chosen
Flash image...
The uploaded image file does not contain a supported format. Make sure that you choose the generic image format for your platform.

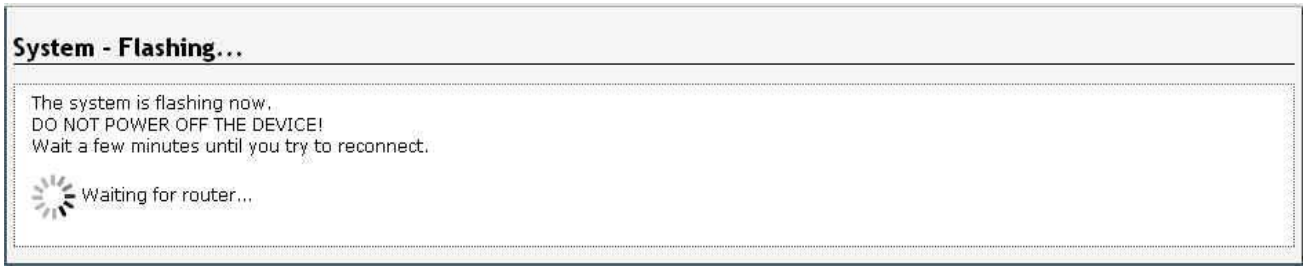
Invalid Image

If image is valid, you will see the checksum and file size. Click “Proceed” to start flash image.


Flash Firmware - Verify
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.
Checksum: 19058383c9cfac793fa392feefa175ce
Size: 3.74 MB
Cancel
Proceed

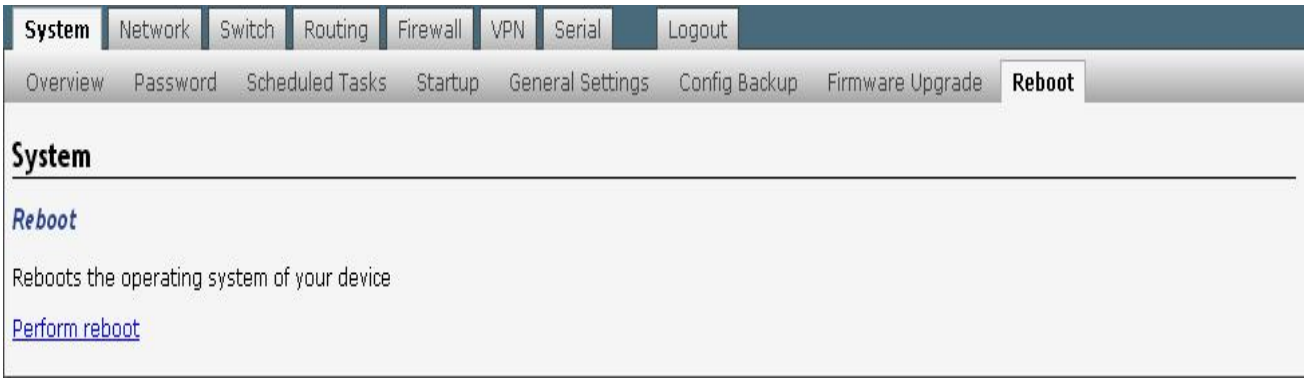
NOTE

- When upgrade complete, the JetBox will reboot automatically. It will connect to web after few minutes.


System - Flashing...
The system is flashing now.
DO NOT POWER OFF THE DEVICE!
Wait a few minutes until you try to reconnect.
Waiting for router...

2-8 Reboot

This page provide user can reboot the JetBox.

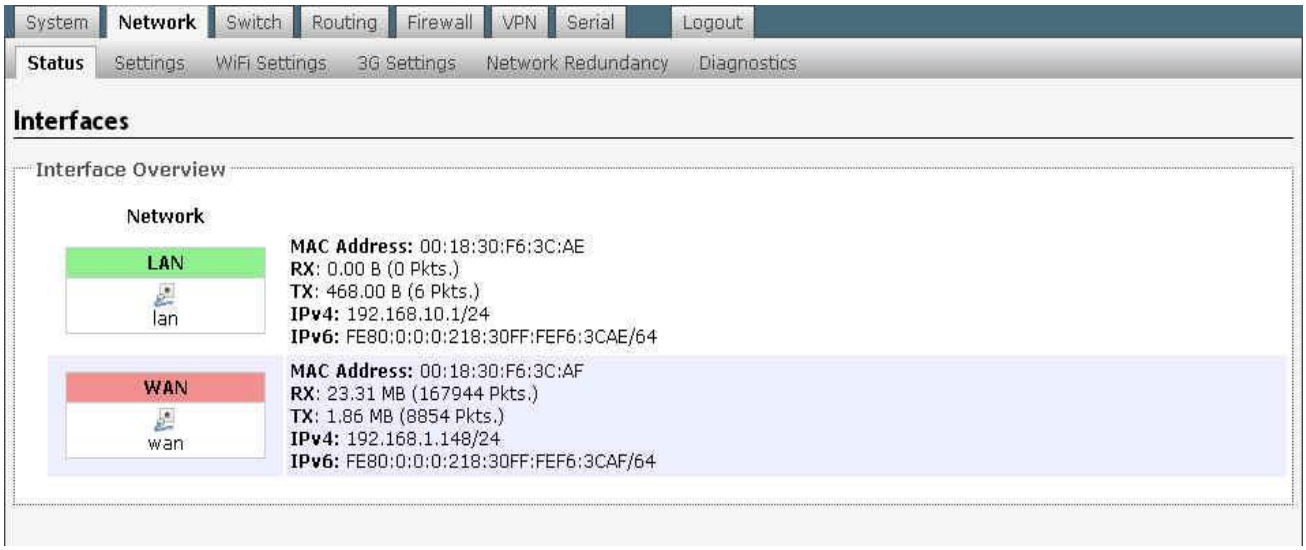


Chapter 3 Network

This chapter includes information about network configuration. The information let user can easily set up the network. We also provide the wireless settings and network redundant function. These features are very useful and important for user.

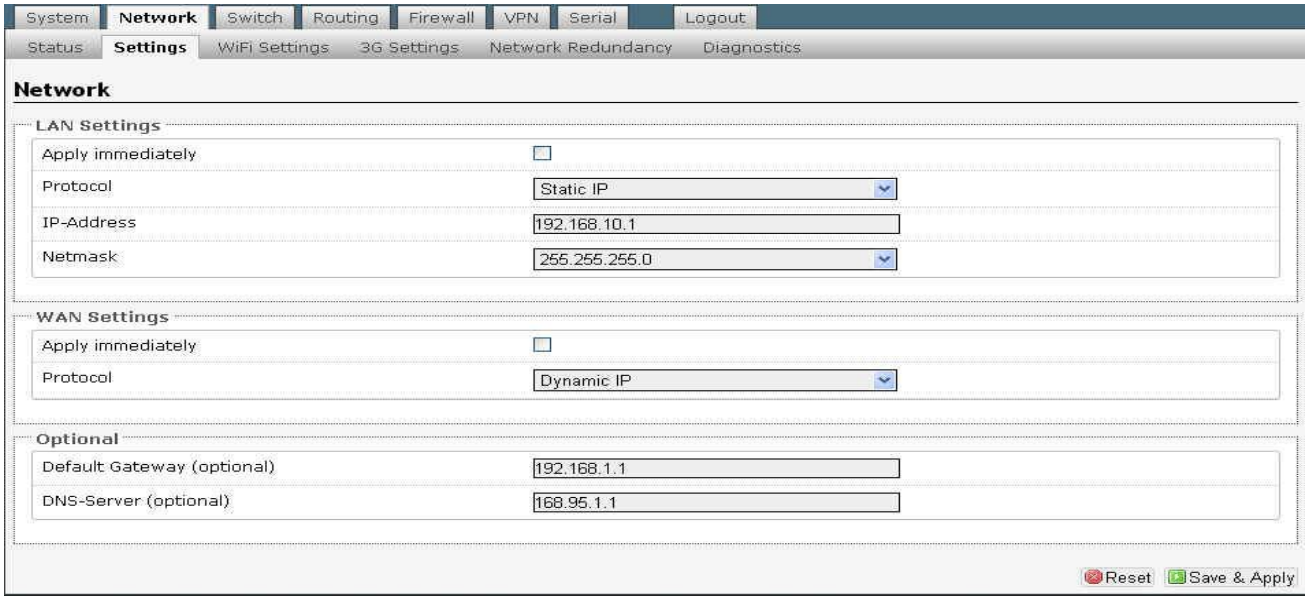
3-1 Status

User can see the detail network information about LAN and WAN.



3-2 Settings

User can change LAN and WAN IP address. It can specify Static IP or Dynamic IP.



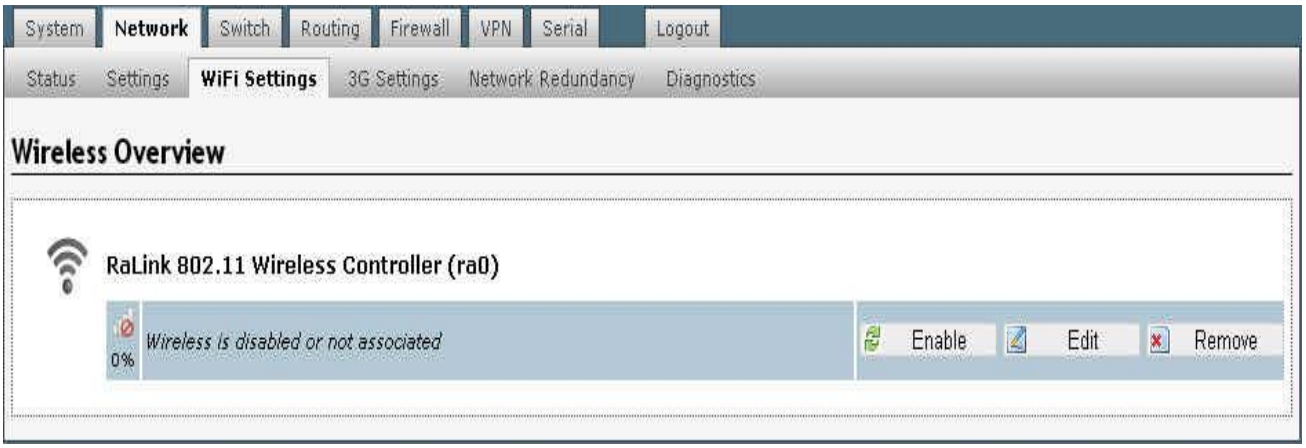
And it also provides two optional fields, Default Gateway and DNS-Server.

- **Apply immediately**

It means that change IP address immediately. If you do not check it, the IP address will change after reboot the JetBox.

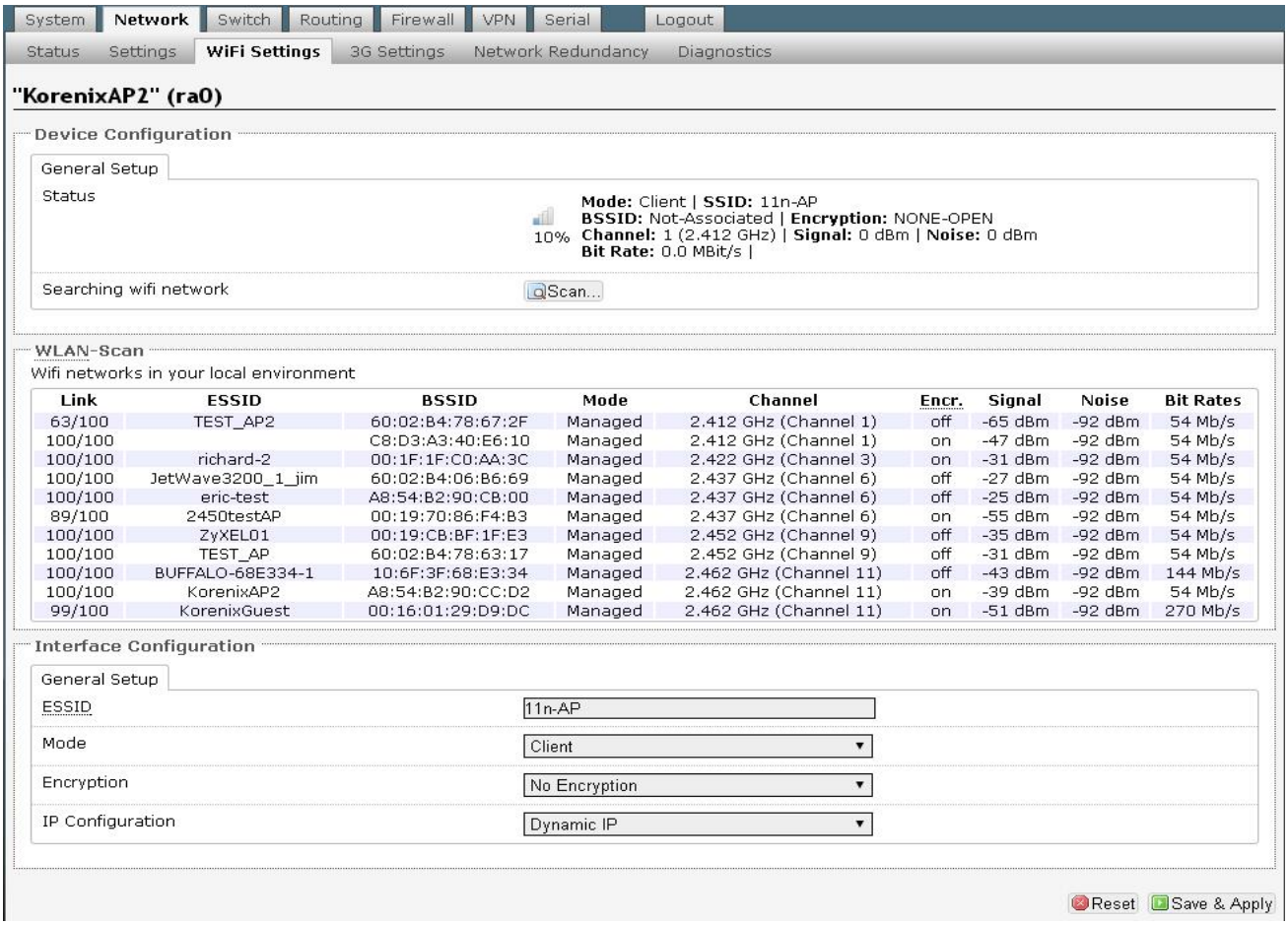
3-3 WiFi Settings

In JetBox5630, we have built-in AWUS036NEH wireless driver. You can easily install and use it to connect Ethernet. When you plug in the wireless dongle, click the WiFi settings and it will show the default wireless interface **ra0**.



Click **Edit** to edit the wireless configuration.

Press “**Scan**” to check how many access point in your environment.


System
Network
Switch
Routing
Firewall
VPN
Serial
Logout
Status
Settings
WiFi Settings
3G Settings
Network Redundancy
Diagnostics
"KorenixAP2" (ra0)
Device Configuration
General Setup
Status
Mode: Client | SSID: 11n-AP
BSSID: Not-Associated | Encryption: NONE-OPEN
10%
Channel: 1 (2.412 GHz) | Signal: 0 dBm | Noise: 0 dBm
Bit Rate: 0.0 MBit/s |
Searching wifi network
Scan...
WLAN-Scan
Wifi networks in your local environment
Link ESSID BSSID Mode Channel Encr. Signal Noise Bit Rates
63/100 TEST_AP2 60:02:B4:78:67:2F Managed 2.412 GHz (Channel 1) off -65 dBm -92 dBm 54 Mb/s
100/100 C8:D3:A3:40:E6:10 Managed 2.412 GHz (Channel 1) on -47 dBm -92 dBm 54 Mb/s
100/100 richard-2 00:1F:1F:C0:AA:3C Managed 2.422 GHz (Channel 3) on -31 dBm -92 dBm 54 Mb/s
100/100 JetWave3200_1_jim 60:02:B4:06:B6:69 Managed 2.437 GHz (Channel 6) off -27 dBm -92 dBm 54 Mb/s
100/100 eric-test A8:54:B2:90:CB:00 Managed 2.437 GHz (Channel 6) off -25 dBm -92 dBm 54 Mb/s
89/100 2450testAP 00:19:70:86:F4:B3 Managed 2.437 GHz (Channel 6) on -55 dBm -92 dBm 54 Mb/s
100/100 ZyXEL01 00:19:CB:BF:1F:E3 Managed 2.452 GHz (Channel 9) off -35 dBm -92 dBm 54 Mb/s
100/100 TEST_AP 60:02:B4:78:63:17 Managed 2.452 GHz (Channel 9) off -31 dBm -92 dBm 54 Mb/s
100/100 BUFFALO-68E334-1 10:6F:3F:68:E3:34 Managed 2.462 GHz (Channel 11) off -43 dBm -92 dBm 144 Mb/s
100/100 KorenixAP2 A8:54:B2:90:CC:D2 Managed 2.462 GHz (Channel 11) on -39 dBm -92 dBm 54 Mb/s
99/100 KorenixGuest 00:16:01:29:D9:DC Managed 2.462 GHz (Channel 11) on -51 dBm -92 dBm 270 Mb/s
Interface Configuration
General Setup
ESSID
11n-AP
Mode
Client
Encryption
No Encryption
IP Configuration
Dynamic IP
Reset
Save & Apply

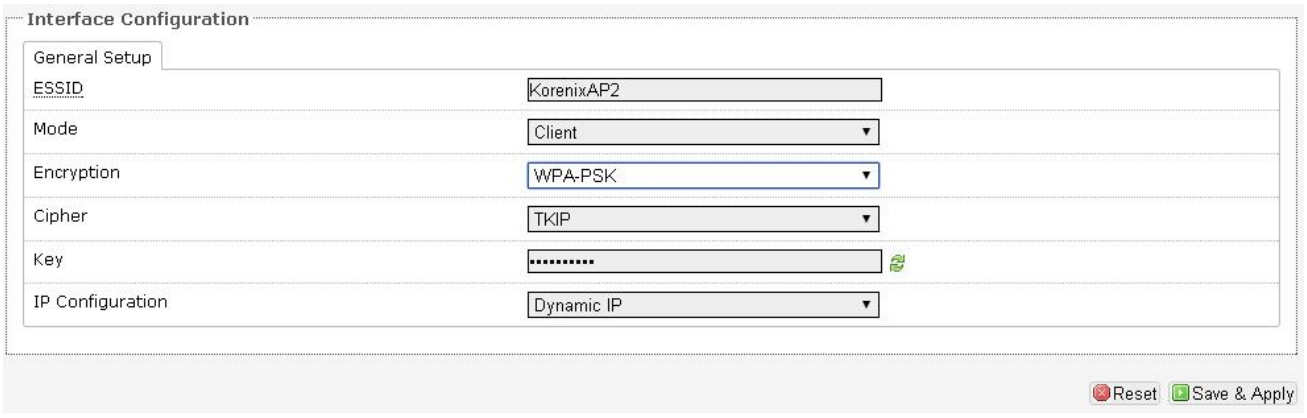
ESSID : Choose your AP name

Mode : We provide Client and Ad-Hoc Mode

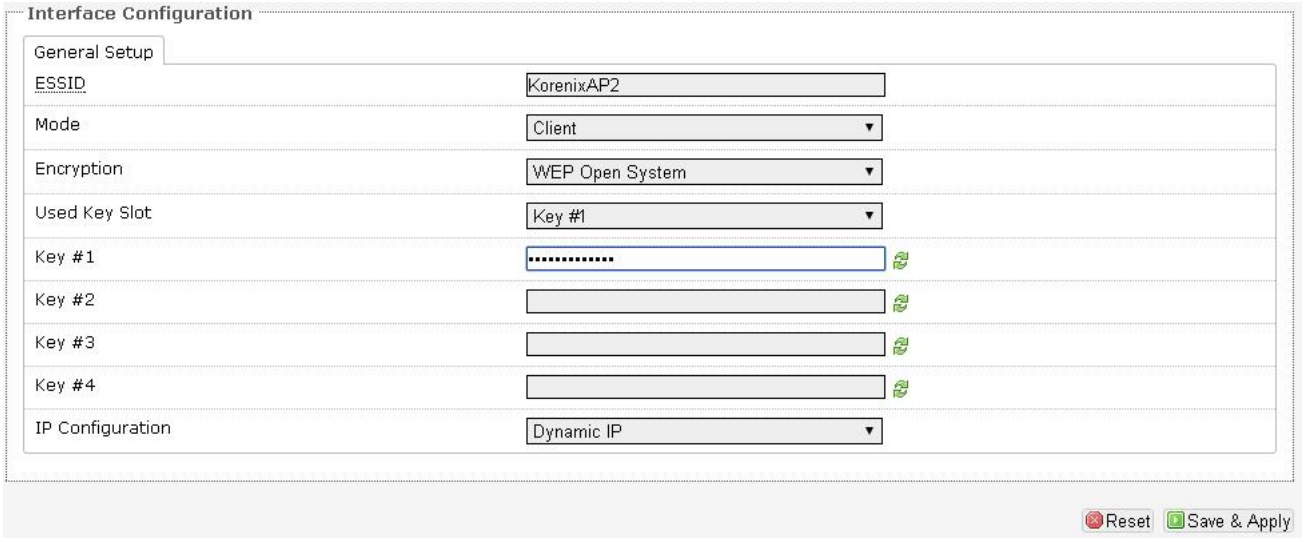
Encryption : Select which encryption mode that you want to connect.

IP Configuration : Select Dynamic IP or Static IP.

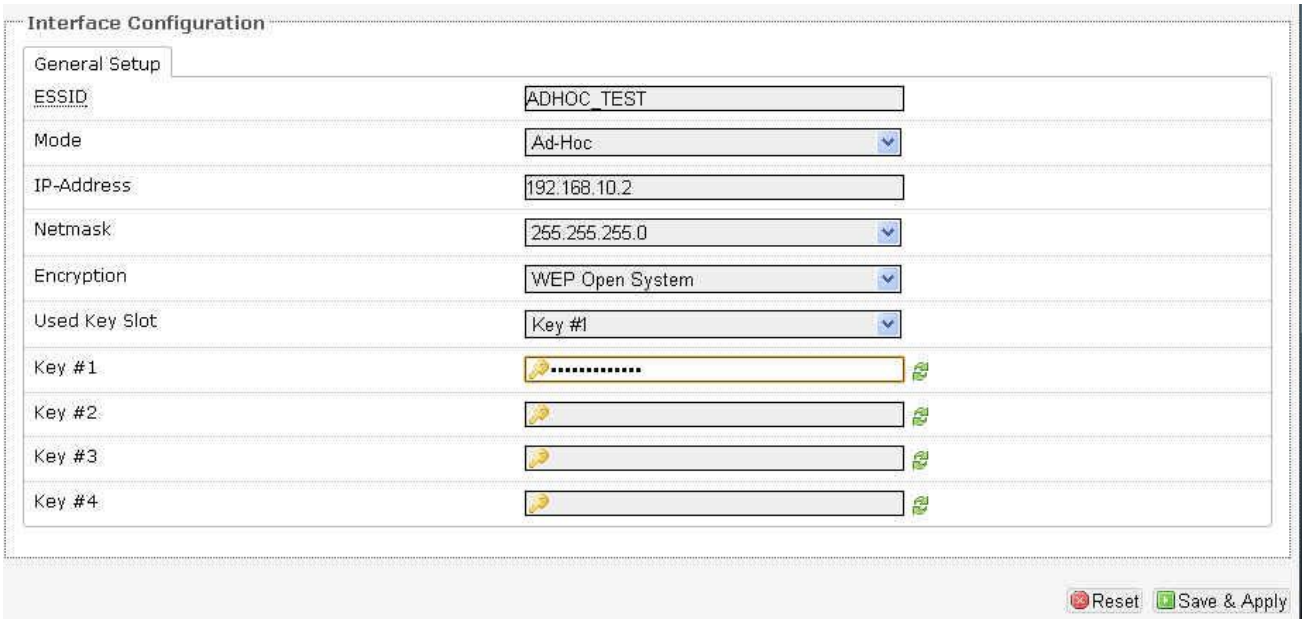
Example: WPA-PSK Mode



Example: WEP Open System Mode



Example: Ad-Hoc Mode



When you select Ad-Hoc mode, you must the IP address to connect another AP.

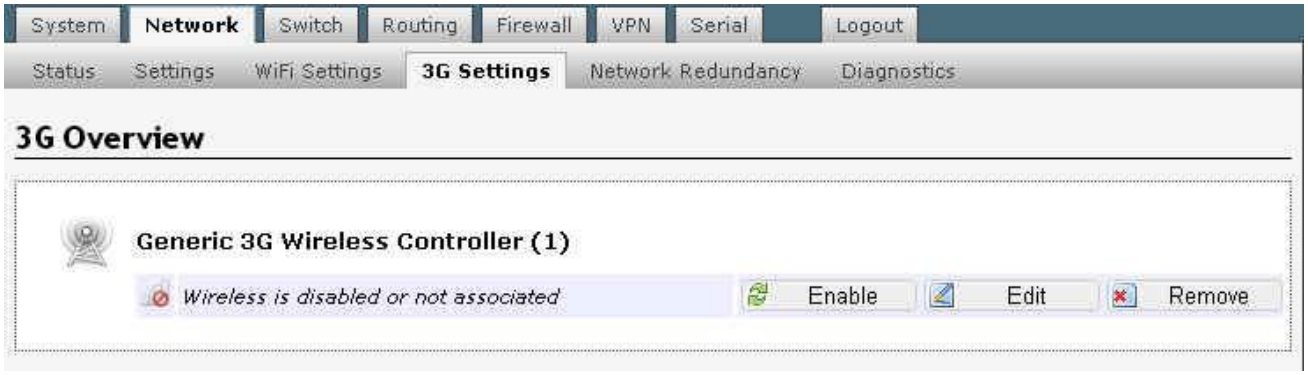
Press **Save & Apply** to save configuration. And go back to WiFi settings page to enable wireless device.

Connect Successfully

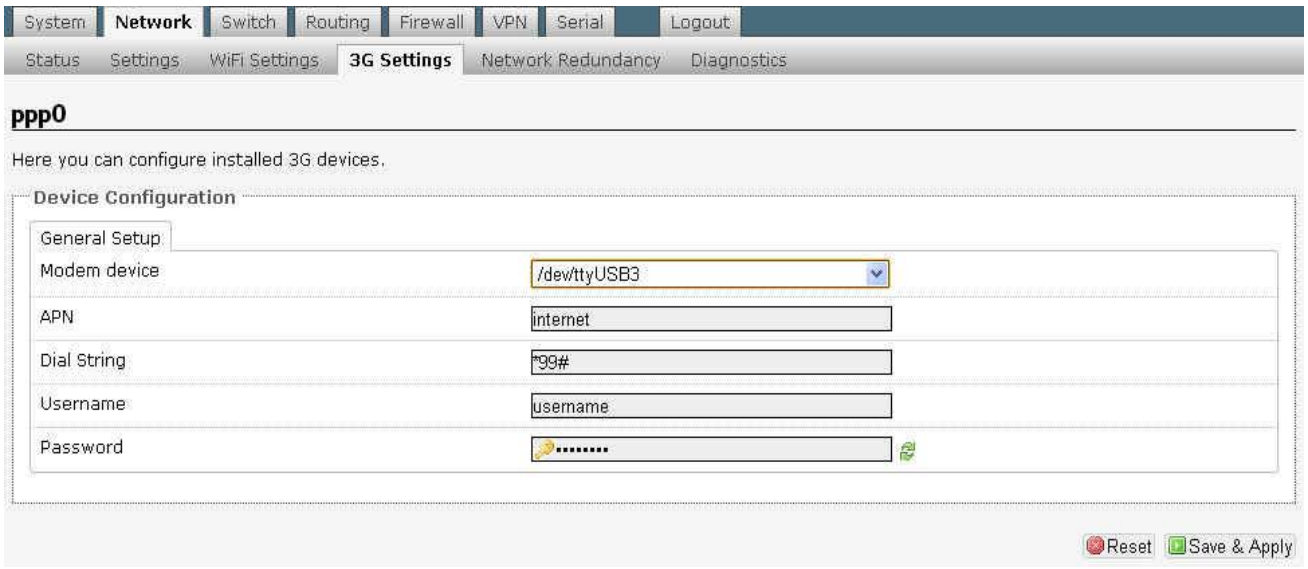
Press **Disable** button to disable wireless device if you don't want to disconnect it

3-4 3G Settings

Plug in the 3G dongle, click the 3G settings and it will show the wireless device.



Click **Edit** to edit the 3G configuration.



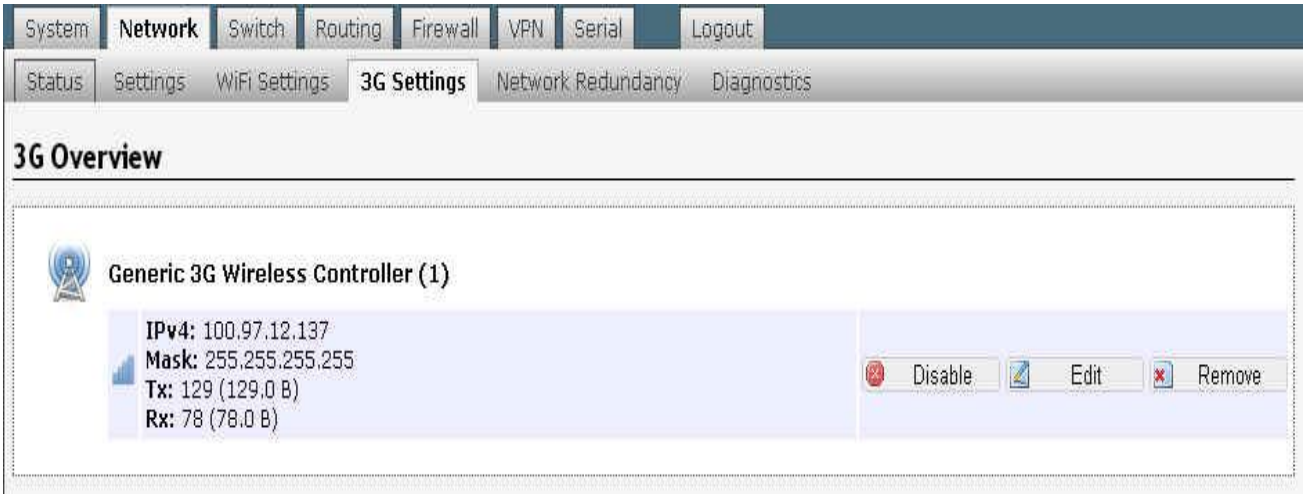
Modem device : The location of the device that **wvdial** should use as your modem.
i.e.: for Sierra MC8092, it uses /dev/ttyUSB3

APN : Specify your APN name. For example, in Taiwan, we use **internet** as APN.

Dial String : Customize to your country or provider for internet connection.
i.e.: in Taiwan, we use ***99#**

Username, **Password** : Change with your username and password if needed.

Press **Save & Apply** to save configuration. And go back to 3G settings page to enable 3G device.

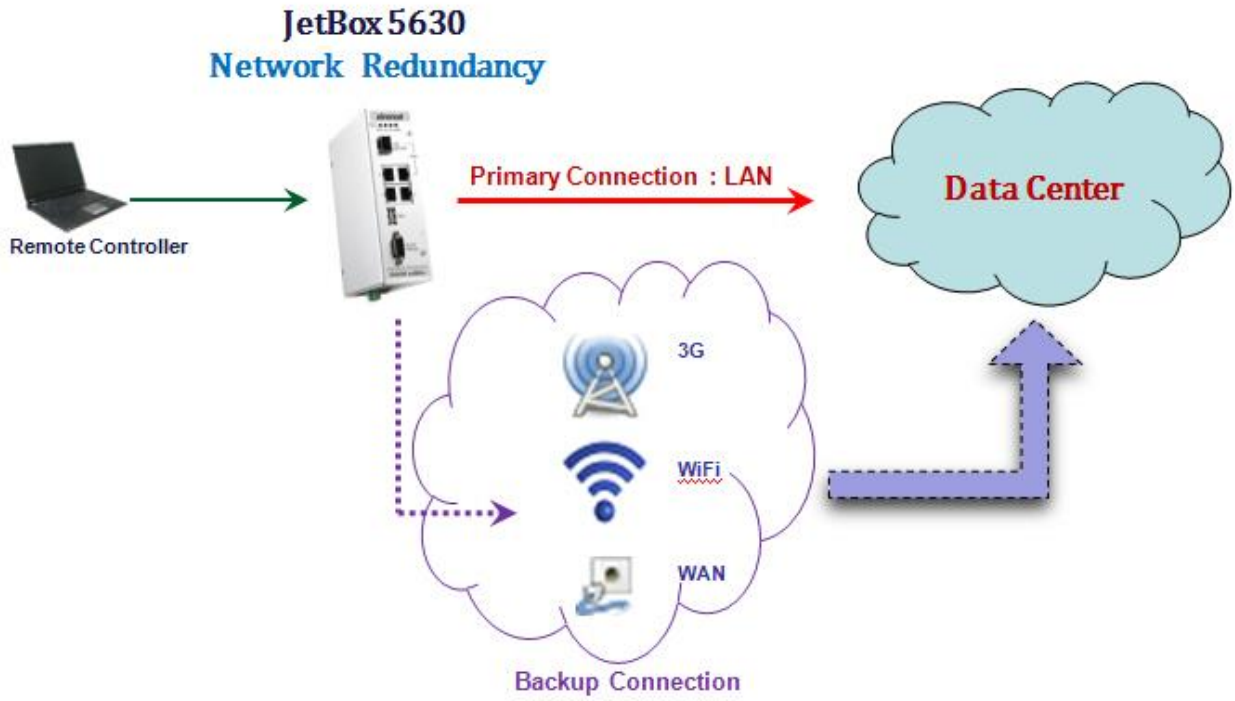


Connect Successfully

Press **Disable** button to disable wireless device if you don't want to disconnect it

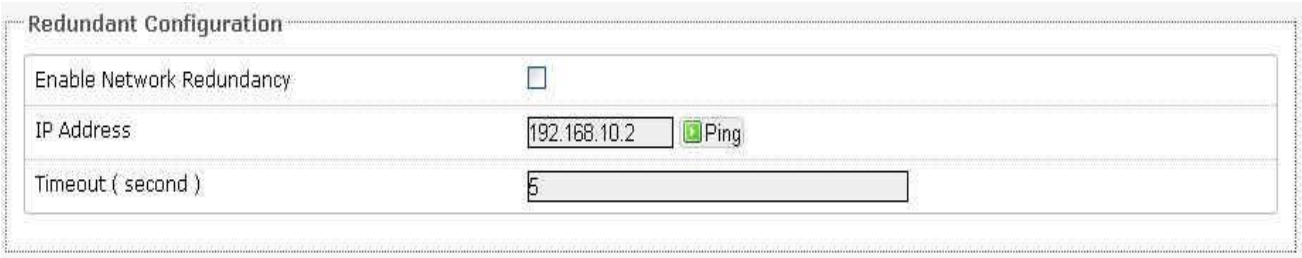
3-5 Network Redundancy

Redundant function checks the link status and the connection integrity. When the primary interface fails, it will switch to the backup WAN (WiFi or 3G) automatically to keep the connection alive.



Choose one of the two following conditions to activate the backup path: 1. Link Check: link down 2. Ping Check: Sends ping commands to a specific IP address

Redundant Configuration



Enable Network Redundancy :

Check it to start network redundancy when you press Save & Apply

IP Address :

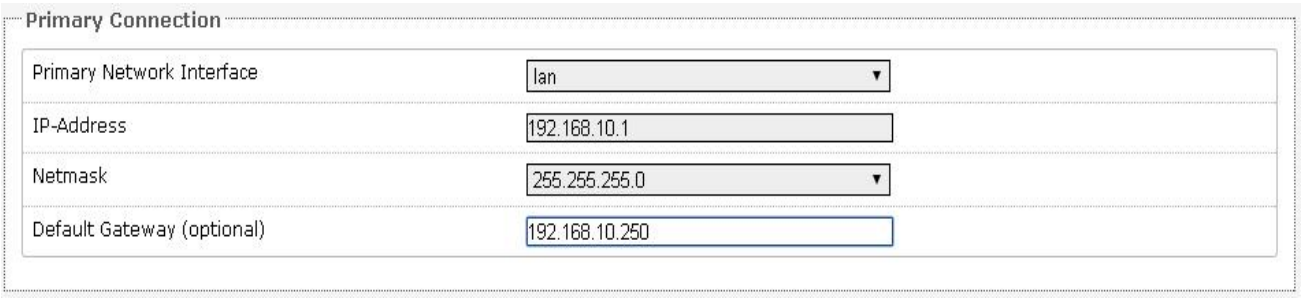
Because we will use IP address field to check link status. So user must to specify it.

And you can check link status by pressing ping.

Timeout (second) :

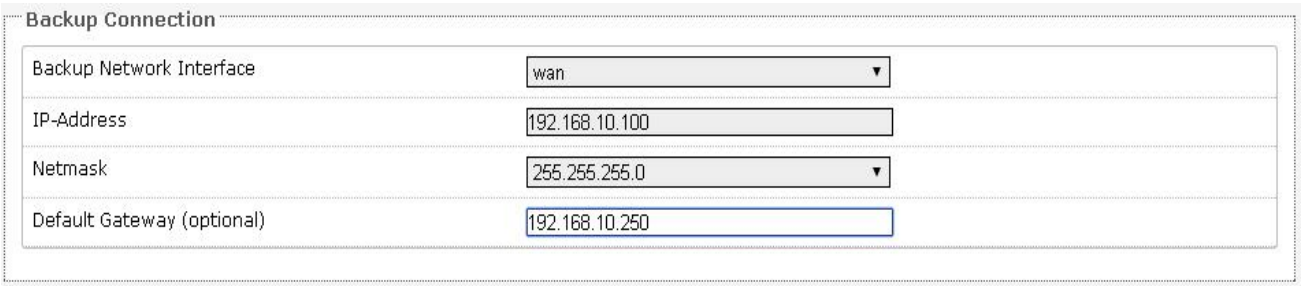
This value means timeout for ping. If it is less, it means switch to backup connection will take less time. Default is 5 seconds.

Primary Connection



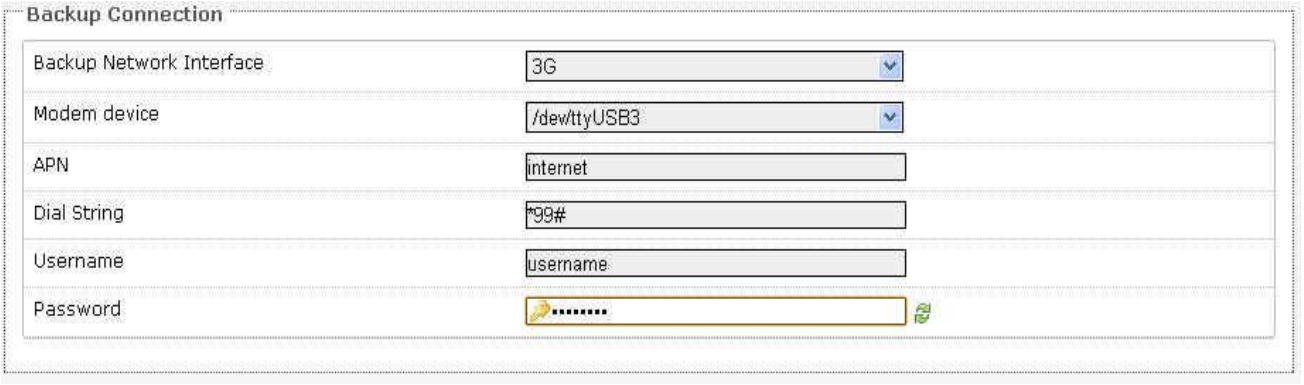
Here user can specify the primary connection and set up its IP address. We support LAN、WAN、WiFi、3G and Other network interface. Usually, LAN or WAN will be specified with primary connection.

Backup Connection



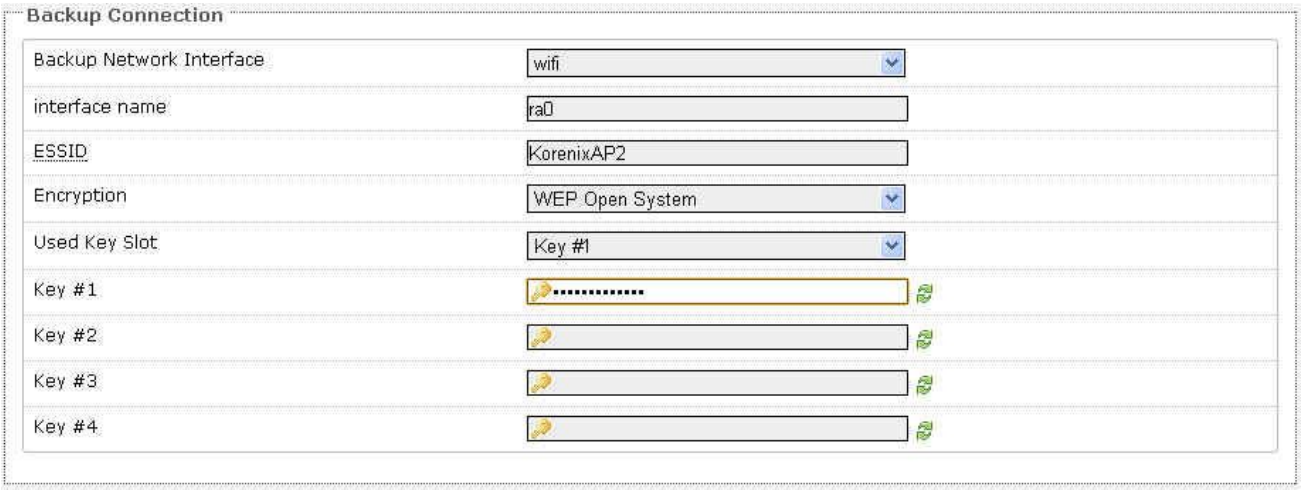
Set up backup connection to make sure the links status can keep alive automatically when primary connection is disconnect. Backup connection can be specified with WiFi or 3G interface.

Backup Connection : 3G interface



When you choose 3G interface for backup connection, you have to specify some settings, like APN, Modem device, Dial String…etc. These settings are the same as network 3G setting.

Backup Connection : WiFi interface



When you choose WiFi interface for backup connection, you have to specify some settings. These settings are the same as network WiFi setting besides interface name. User has to specify WiFi interface name to make sure that we can use right interface to connect.

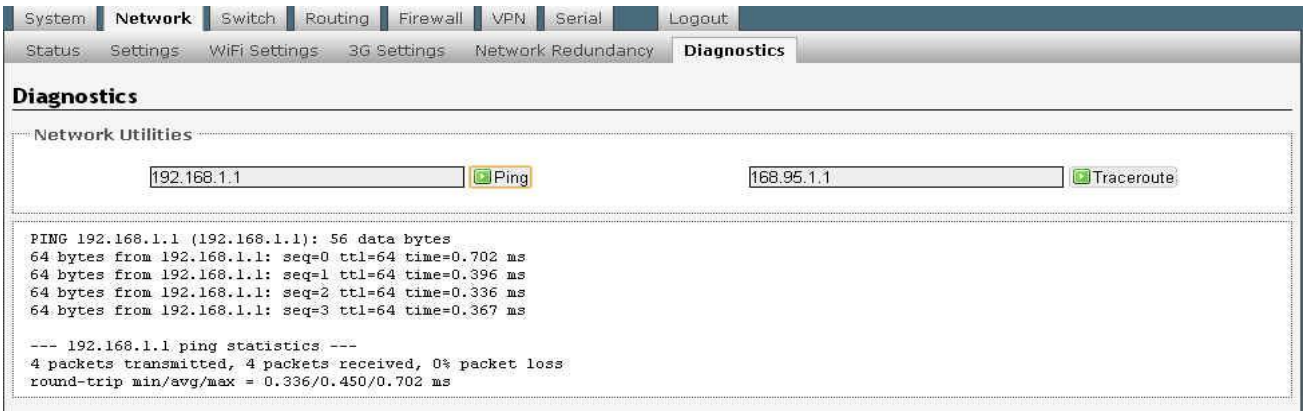
After all setting, click “Save&Apply” to start Network Redundancy function.

NOTE

- If primary and backup connection can’t connect to server both, we will disable redundant daemon after retry 10 times.

3-6 Diagnostics

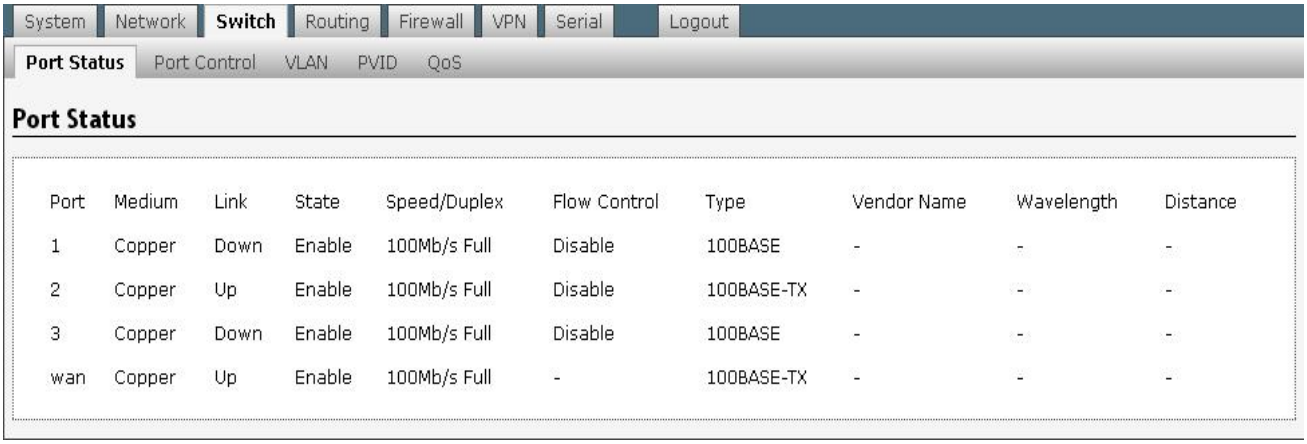
We provide a network diagnostic tool to verify network connection. User can use ping or traceroute function to check it



Chapter 4 Switch

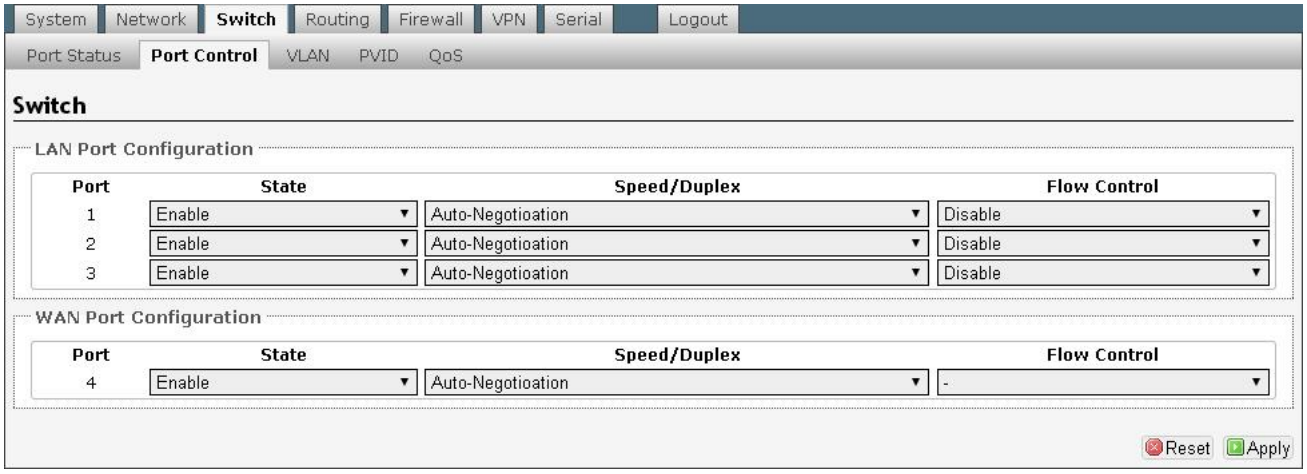
In this chapter, we explain how to configure JetBox network configuration via web interface.

4-1 Port Status



Here, you can see the all ports status of JetBox 5630 series.

4-2 Port Control



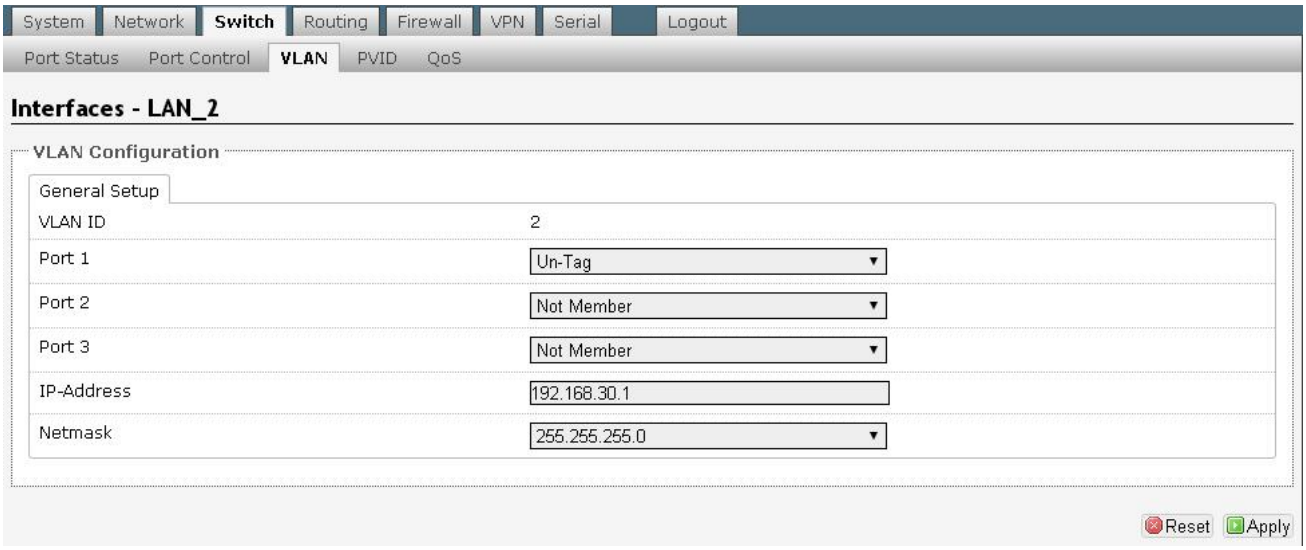
You can set up the each port configuration. Just like ethtool command in JetBox console.

NOTE

1. To change SFP speed you need to reboot the system to make it effective.
2. Please make sure the spec of SFP matching with the SFP speed setting, or exception conditions would happen.

4-3 VLAN

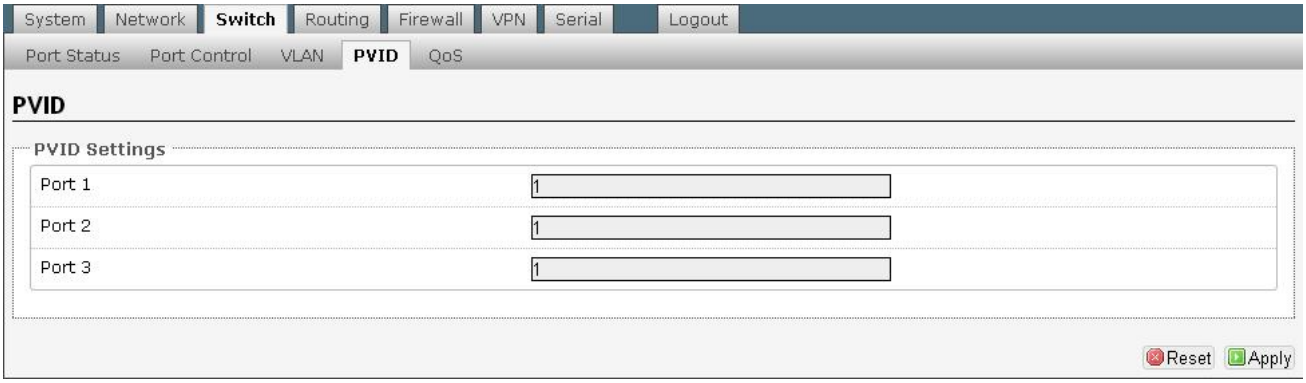
You can add or delete vlan interface via web. Just like vconfig command in JetBox console.



Here, you also can directly specify IP address of vlan interface.

Back to VLAN setting page, you can press Enable button to link up the vlan interface. And the IP address will be set automatically according to settings.

4-4 PVID



User can change port's pvid via web. It is the same as "ethtool -P" command.

4-5 QoS

In the past, the concept of quality in networks meant that all network traffic was treated equally. The QoS (Quality of Service) concept means that some traffic needs preferential treatment because the requirements of some applications and users are more critical than others. In addition, QoS for networks is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications.

When QoS is enabled, packets are queued based on the port trust mode, which is derived from the incoming port configurations, CoS queue mapping, or DSCP queue mapping.

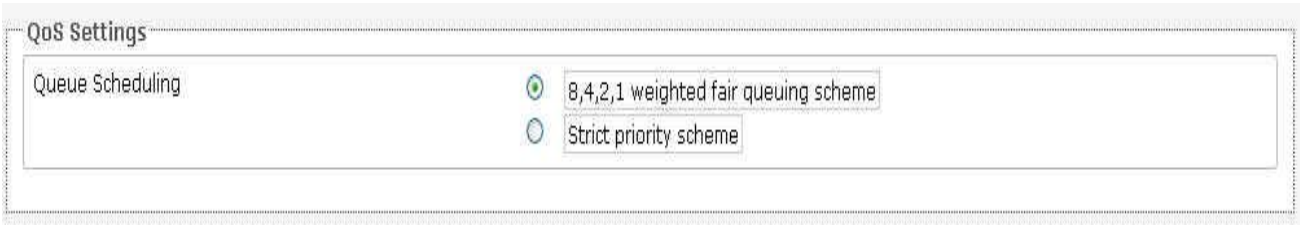
Through this section, you can set up the priority level for port based CoS value, incoming CoS (CoS-Queue Mapping), or incoming DSCP (DSCP-Queue Mapping) and define the way to process all ingress packets by either the strict priority scheme or the weighted fair queue according to the priority levels of port based, CoS only, DSCP only, CoS first, or DSCP first. JetBox 5630 supports 4 physical queues from 0 to 3.

Queue scheduling

Use an 8,4,2,1 weighted fair queuing scheme: This is also known as WRR (Weight Round Robin). JetBox 5630 follows the rate of 8:4:2:1 to process the packets with the high, the medium, the low, and the normal priority in a queue. For example, the system processes 8 packets with the high priority in the queue, 4 with medium priority, and 2 with low priority and 1 with the normal priority at the same time.

Use a strict priority scheme: Packets with higher priority in the queue will always be processed first, unless there is no packet with higher priority in a queue.

The default is using an 8,4,2,1 weighted fair queuing scheme.



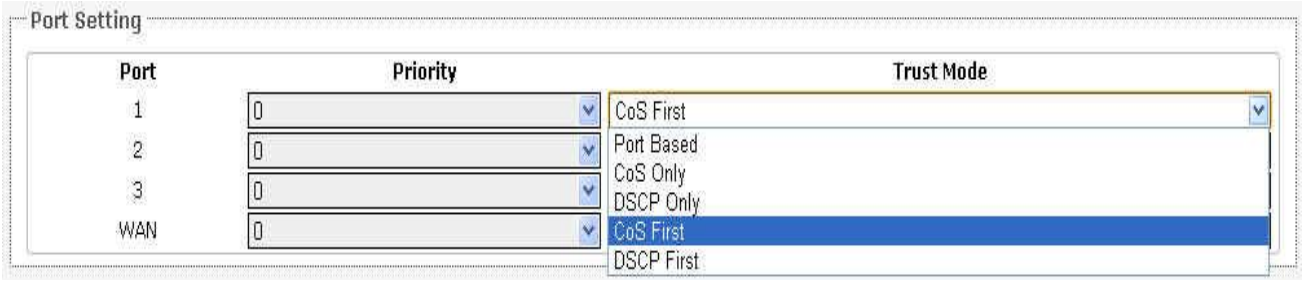
Port setting

Priority:

You can choose the QoS priority levels for each Ethernet port of JetBox 5630 from 0 to 7.

Trust Mode	Description
Port Based	Use the priority level of the port configuration
CoS Only	Use the priority level of CoS Queue Mapping only
DSCP Only	Use the priority level of DSCP Queue Mapping only
DSCP First	Use the priority level of both CoS and DSCP Queue Mapping, but DSCP Queue Mapping first
CoS First	Use the priority level of both CoS and DSCP Queue Mapping, but CoS Queue Mapping first

Trust Mode



JetBox 5630 will give all ingress packets the priority tag based on the priority level (CoS Value) of the ingress port. The CoS value maps to physical queue in the page of CoS Queue Mapping.

CoS Value	Traffic Type
0	Best effort
1	Background
2	Standard
3	Excellent load

CoS (Class of Service): Layer 2 prioritization of packets is based on a CoS value.

4	Controlled load
5	Voice and Video
6	Layer 3 network control reserved traffic
7	Layer 2 network control reserved traffic

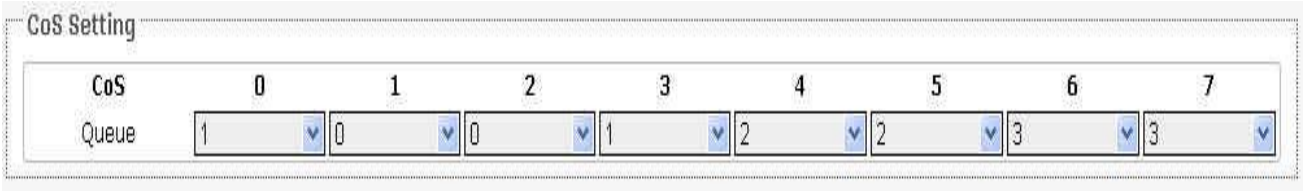
QoS priority level follows 802.1p

CoS-Queue Mapping

The default setting follows IEEE802.1p standard to map the CoS values to the physical queues. You can modify the physical queue of each item here.

CoS Value	Physical	Queue
0	Normal	1
1	Low	0
2	Low	0
3	Normal	1
4	Medium	2
5	Medium	2
6	High	3
7	High	3

The CoS values map to the physical queues



DSCP (Differentiated Services Code Point): Layer 3 prioritization of packets is based on a DSCP value. A network could have from 0 to 64 different traffic classes using different markings in the DSCP.

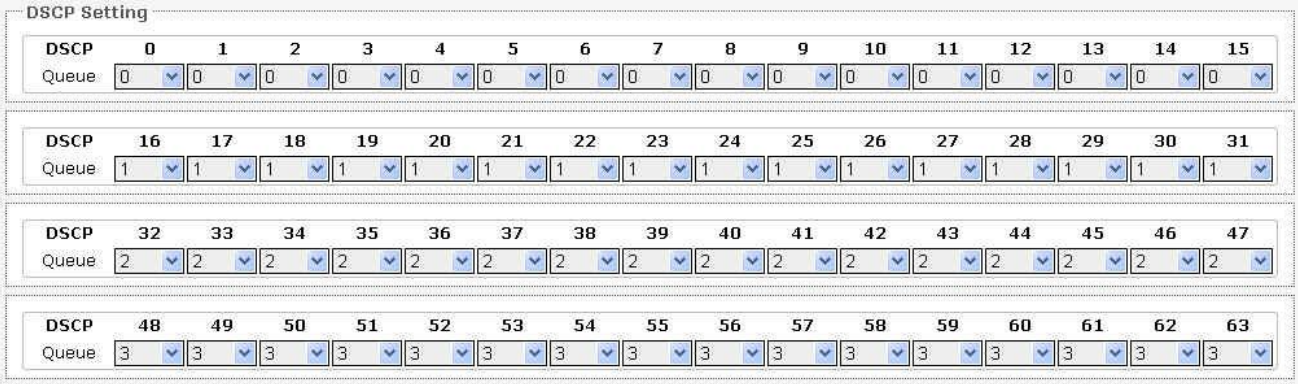
DSCP-Queue Mapping

The default setting follows IEEE802.1p standard to map the DSCP values to the physical queues. You can modify the physical queue of each item here.

DSCP Value	Physical	Queue
0~15	Low	0
16~31	Normal	1
32~47	Medium	2

48~63	High	3

The DSCP values map to the physical queues

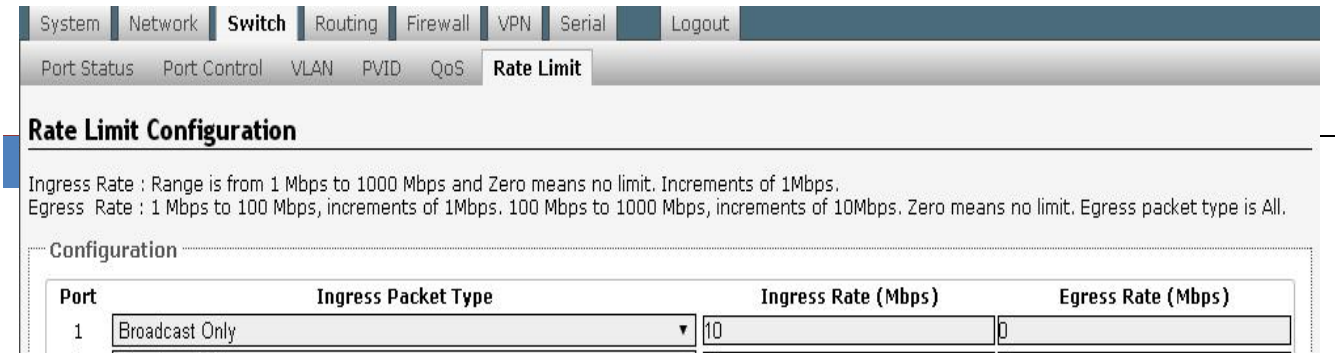


It is the same as ethtool -q and ethtool -Q command in JetBox console. As below

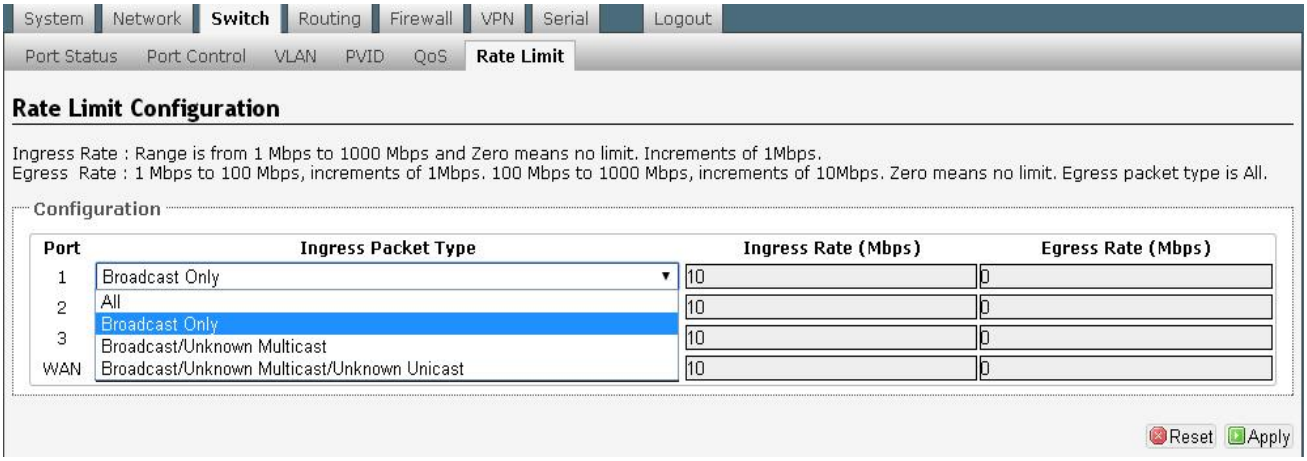
```
~ $ ethtool -q lan:1
Queue Scheduling:
        8,4,2,1 weighted fair queuing

Port Setting:
        Port 1   : CoS First, Priority : 0
        Port 2   : CoS First, Priority : 0
        Port 3   : CoS First, Priority : 0
        Port WAN : CoS First, Priority : 0

IEEE Tag CoS Mapping:
        Queue 0:1,2,
        Queue 1:0,3,
        Queue 2:4,5,
        Queue 3:6,7,

IP DSCP Mapping:
        Queue 0:
00,01,02,03,04,05,06,07,08,09,10,11,12,13,14,15,
        Queue 1:
16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,
        Queue 2:
32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,
        Queue 3:
48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,
```

4-6 Rate Limit

Rate limiting is used to control the rate of traffic that is sent or received on a network interface. For ingress rate limiting, traffic that is less than or equal to the specified rate is received, whereas traffic that exceeds the rate is dropped. For egress rate limiting, traffic that is less than or equal to the specified rate is sent, whereas traffic that exceeds the rate is dropped.


System Network Switch Routing Firewall VPN Serial Logout
Port Status Port Control VLAN PVID QoS Rate Limit
Rate Limit Configuration
Ingress Rate : Range is from 1 Mbps to 1000 Mbps and Zero means no limit. Increments of 1Mbps.
Egress Rate : 1 Mbps to 100 Mbps, increments of 1Mbps. 100 Mbps to 1000 Mbps, increments of 10Mbps. Zero means no limit. Egress packet type is All.
Configuration
Port
Ingress Packet Type
Ingress Rate (Mbps)
Egress Rate (Mbps)
1
Broadcast Only
10
0

Ingress Packet type : Select the packet type that you want to filter. The packet types have all types of packets, Broadcast Only, Broadcast/Unknown Multicast, and Broadcast/Unknown Multicast /Unknown Unicast packets.



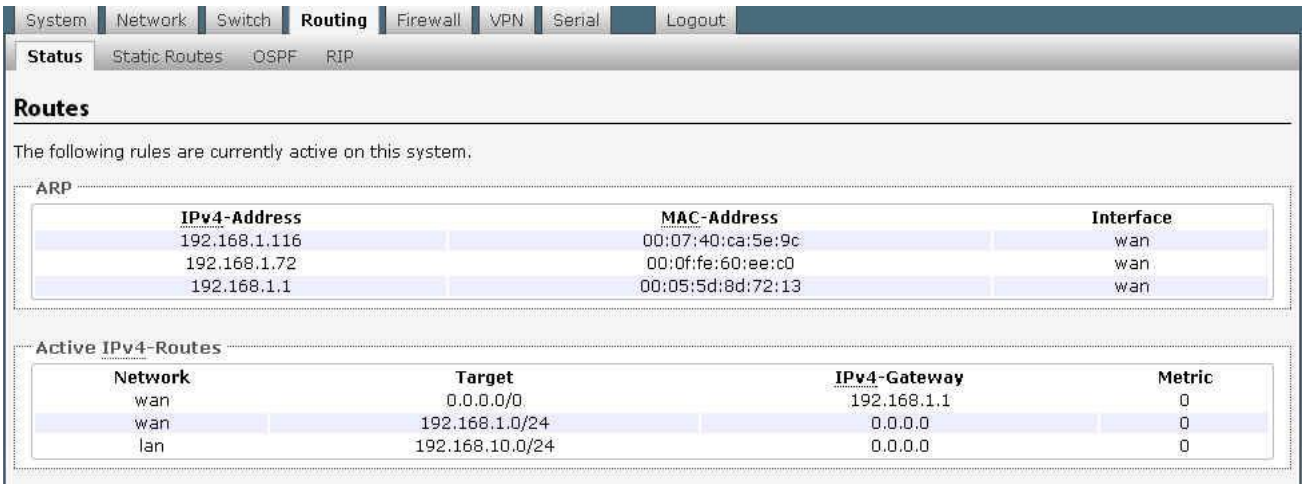
Ingress Rate (Mpbs) : Ingress rate in Mbps, the rate range is from 1 Mbps to 1000 Mbps, increments of 1Mbps. Zero means no limit. The default ingress rate is ''10 Mbps''.
Egress Rate (Mpbs) : Egress rate in Mbps, the rate range is from 1 Mbps to 100 Mbps, increments of 1Mbps. 100 Mbps to 1000 Mbps, increments of 10Mbps. Zero means no limit. The default egress rate is ''no-limit''. Egress rate limiting has an effect on all types of packets, including unicast, multicast and broadcast packets.

Chapter 5 Routing

In this chapter, we provide users how to configure JetBox routing configuration via web interface. We support Static routes、OSPF and RIP routing protocol.

5-1 Status

Check routing status and you also can see ARP table.



5-2 Static Routes

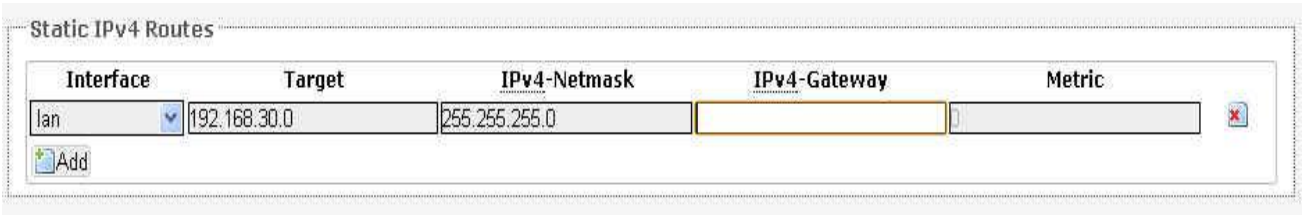
You can add static route with this page.

For example, we want to add a rule

route add -net 192.168.30.0 netmask 255.255.255.0 gw 192.168.10.1

```
~ $
~ $ route add -net 192.168.30.0 netmask 255.255.255.0 dev lan
~ $
~ $ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     *               255.255.255.0   U     0      0        0 lan
192.168.20.0    *               255.255.255.0   U     0      0        0 wan
192.168.30.0    *               255.255.255.0   U     0      0        0 lan
~ $
```

In web, you can set up as below

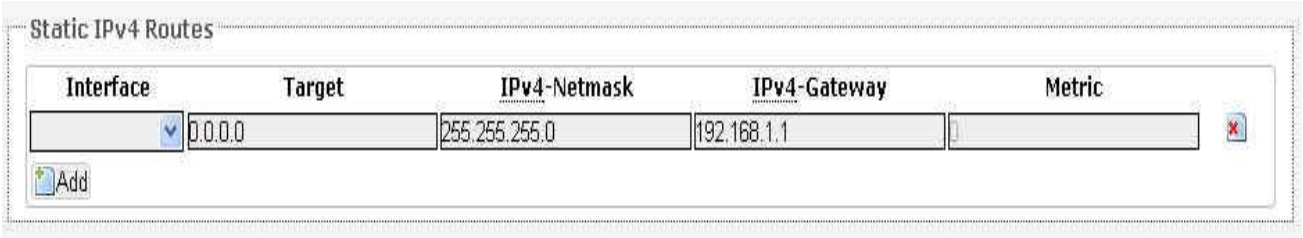


In JetBox console, add default gateway

route add default gw 192.168.1.1

```
~ $ route add default gw 192.168.1.1
~ $
~ $ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    0      0        0 lan
192.168.1.0     *               255.255.255.0   U     0      0        0 lan
192.168.20.0    *               255.255.255.0   U     0      0        0 wan
192.168.30.0    *               255.255.255.0   U     0      0        0 lan
~ $
```

In web, you can set up as below

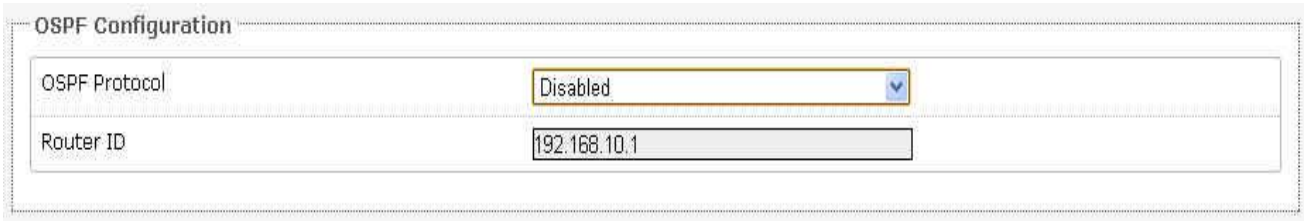


5-3 OSPF

The OSPF is short of the Open Shortest Path First.

OSPF is a link-state protocol. The Link is an interface on the router, it equips the IP, mask, the type of network, the routers connected to that network. The State is its relationship to its neighboring routers. The Metric is the distance between the 2 links, it is usually the bandwidth of the link in link-state protocol. The Link State Database is the collection of all these link states. The destination network address, the shortest metric to the network and the IP address of the next hop are specified in the link state database.

OSPF Configration



OSPF Protocol : You can Enabled or Disabled OSPF protocol after press ”Apply” button.

Router ID : The router ID can be any IP address, however, the IP address of the existed local interface is suggested. With such IP address, you can find the router/switch easier

Routing For Networks

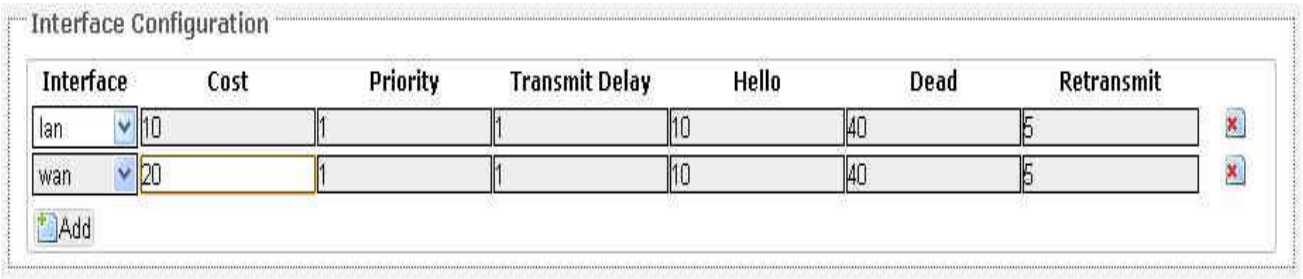
Type the network address and the Area ID in the field. Click “Add” to apply the setting. You can see the network table in below.

NOTE

All the Area ID of the router/switch within the same area should use the same ID. All the network address should be added.

Interface Configuration

This page allows user to specify parameters of each interface.



Interface: The Interface name.

Cost: The distance of this link/Interface, the default is identified depends on what the bandwidth is by the system. The value can be changed to decide the best router.

Priority: The priority of this link/Interface. Set priority to help find the OSPF designated router for a network. The default is 1. The range is 0 to 255.

Transmit Delay: The transmit delay timer of this link/Interface. Transmit Delay is the estimated number of seconds to wait before sending a link state update packet. The default value is 1 second.

Hello: The Hello timer of this link/Interface. The value must be the same for all routers/switches on a network. The default value is 10 seconds. The min. value is 1.

Dead: The Dead Interval Timer of this link/Interface. The Dead timer is the time to identify whether the interface is down or not before the neighbors declare the OSPF router to be down. The default value is 4 times (40 seconds) than the Hello interval (default is 10).

Retransmit: The count of Retransmit of this link/Interface. The Retransmit time specifies the number of seconds between link state advertisement transmissions. The default value is 5 seconds.

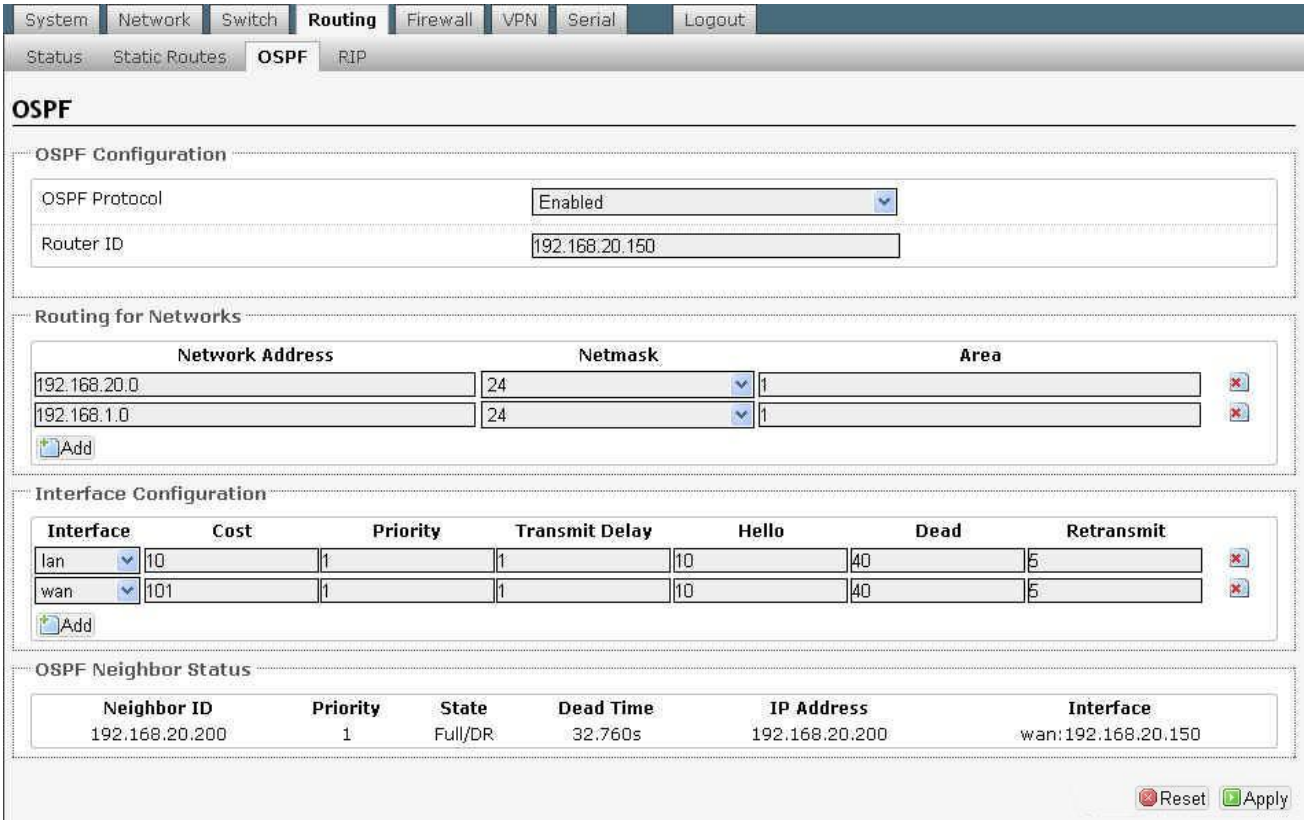
OSPF Neighbor Status

This section allows user to see the OSPF Neighbor information.

Below is the example of a simple OSPF environment. The Hello packets are exchanged between the switch to next switches. While the State is changed to “Full”, that means the

exchange progress is done. The Neighbor ID is the Router ID of the Neighbor routers/switches. The Priority is the priority of the link. The Dead Time is the activated time of the link. There are one interface attached the switch you check. The IP address shows the learnt IP interface of the next hops. And the Interface shows the connected local interface.

Once you finish configuring the settings, click “Apply” to apply your configuration.



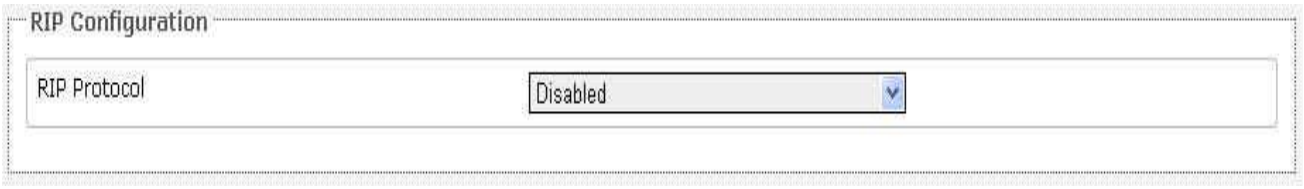
5-4 RIP

The RIP is short of the Routing Information Protocol. RIP was in widespread use years before it was standardized in as RFC 1058 in 1988. Version 2 of RIP was completed in 1994.
RIP is the most known Distance Vector type dynamic routing protocol, or known as Hop Based routing protocol. It uses hop count as a distance metric, each router advertises its routing table every 30 seconds. The maximum routers RIP can support is 15, the 16th router represents Infinity.

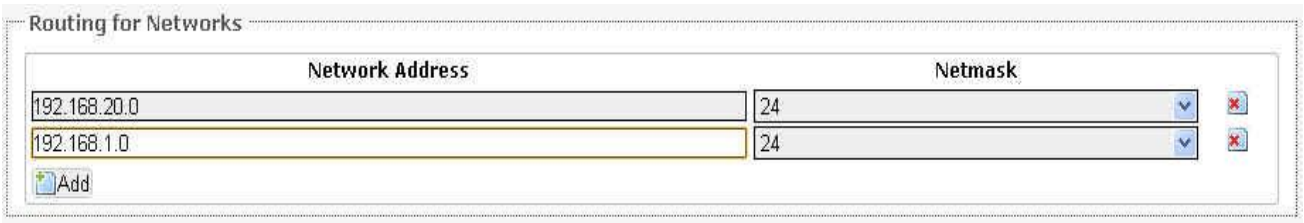
RIP Configuration

This page shows how to configure RIP protocol.

RIP Protocol: Enabled or Disabled OSPF protocol after press ”Apply” button.

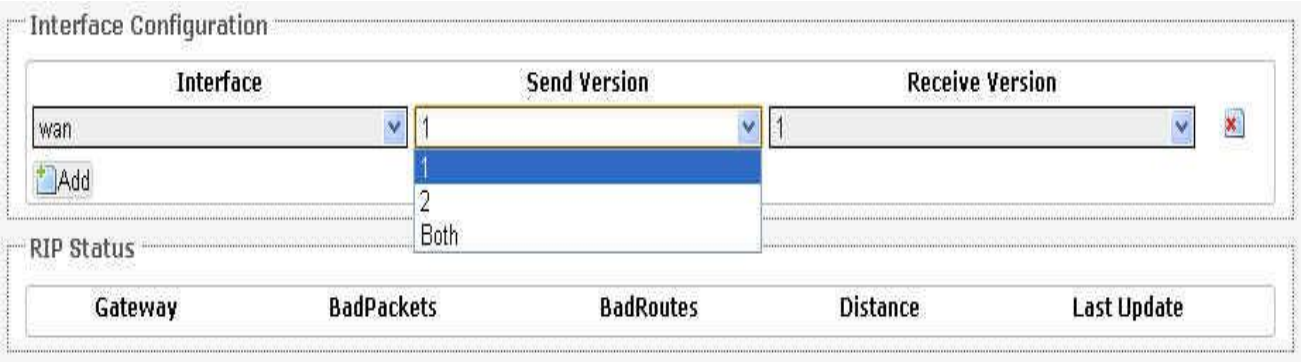


Routing for Networks: All the networks no matter directly connected or learnt from other router/switch should be added to the switch. The format is IP Network/bit mask.



RIP Interface Configuration

In RIP Interface Configuration, you can configure Send Version and Receiver Version. Select the RIP Version of the interface. Once you finish configuring the settings, click on “Apply” to apply your configuration.



RIP Status

This section allows user to see the RIP Neighbor information.

Once you finish configuring the settings, click “Apply” to apply your configuration.

Chapter 6 Firewall

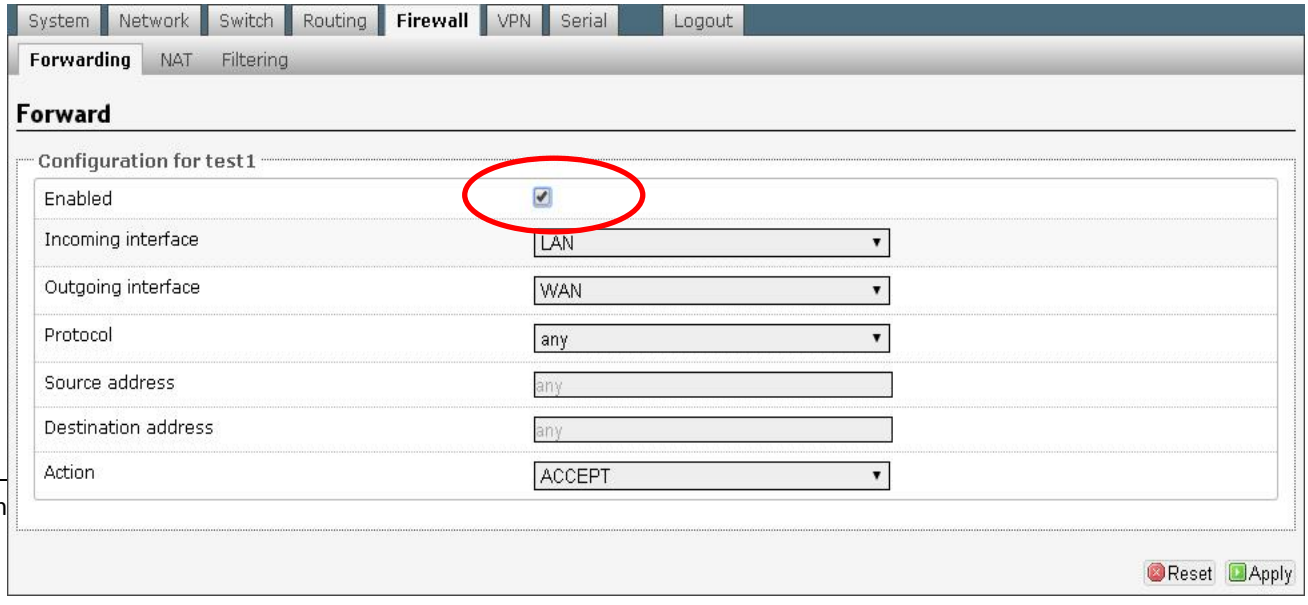
It is the same as iptables command in JetBox console. In web interface, we provide three basic functions for user to set up firewall in Linux.

6-1 Forwarding

The FORWARD policy allows an administrator to control where packets can be routed within a LAN. For example, to allow forwarding for the entire network, the following rules can be set:
In JetBox command :
iptables -A FORWARD -i lan -o wan -j ACCEPT

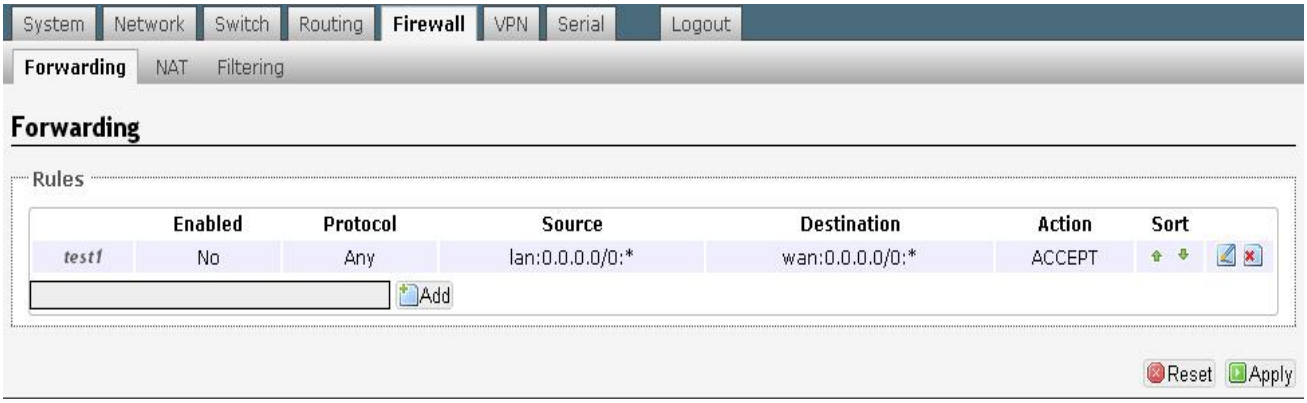
```
~ $ iptables -A FORWARD -i lan -o wan -j ACCEPT
~ $ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
~ $
```

In web interface, you can specify as below



Click on “Enabled” and it will apply this rule immediately after press “Apply”

Back to Forwarding page, you can see a rule that you had added.



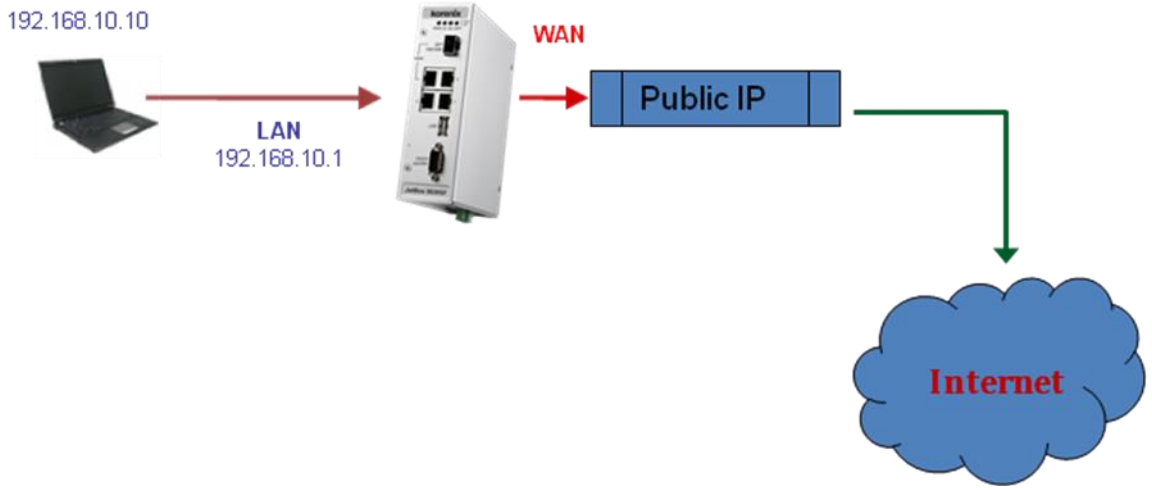
If you want to delete the rule, just click delete button and press “Apply”.

6-2 NAT

Network address translation (NAT) is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping one IP address space into another.

Postrouting and IP Masquerade

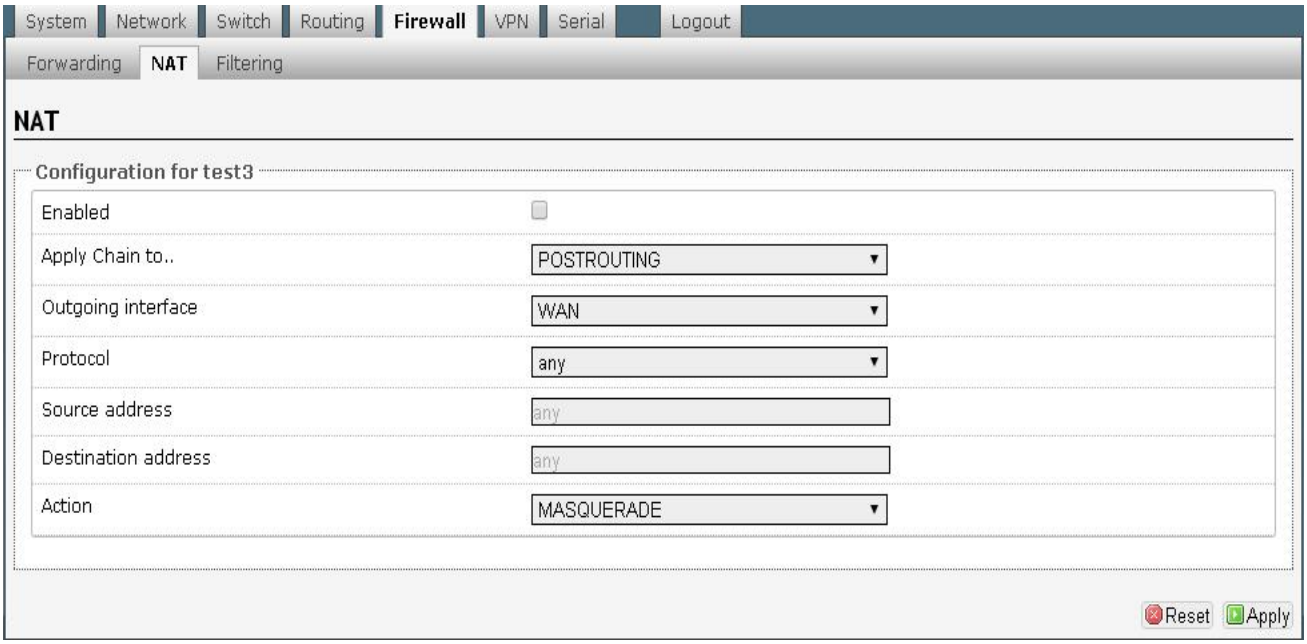
Masquerade allow LAN nodes with private IP addresses to communicate with external public networks.



iptables command :

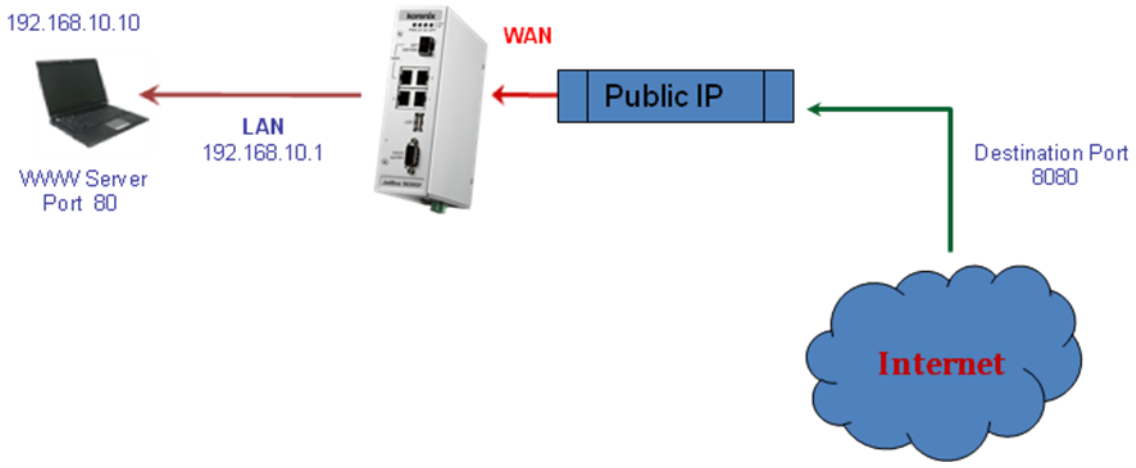
iptables -t nat -A POSTROUTING -o WAN -j MASQUERADE

In Web interface



DNAT and Prerouting

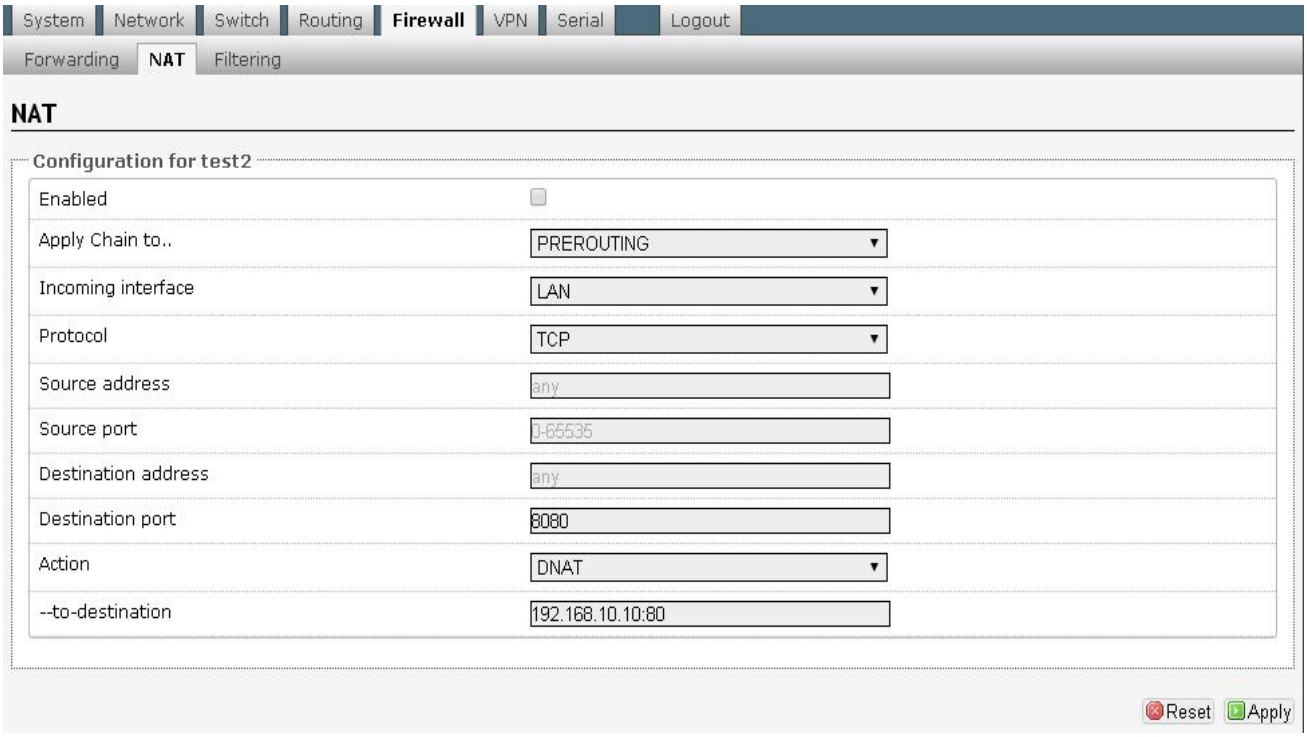
Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an en route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet.



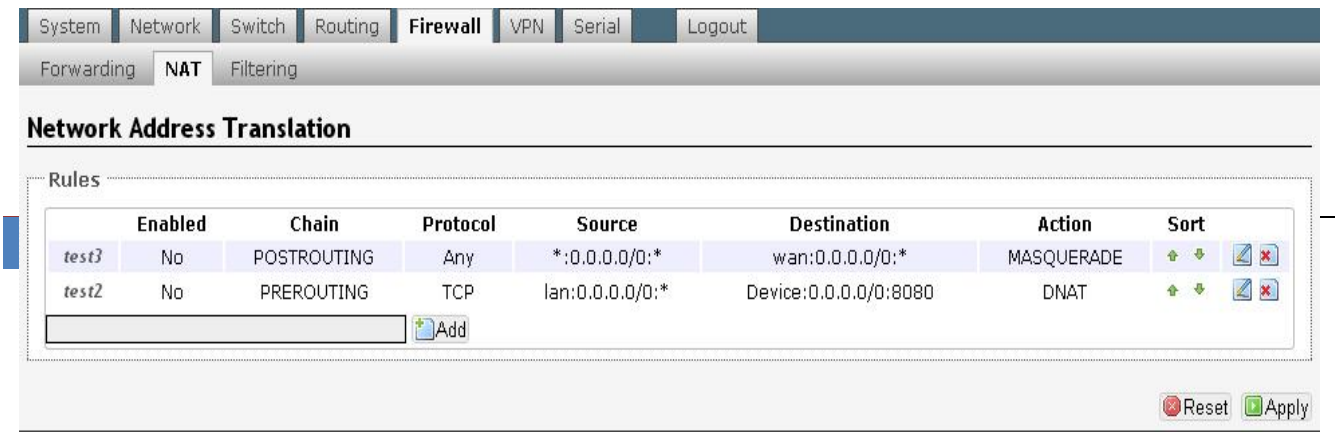
iptables command :

iptables -t nat -A PREROUTING -p tcp -i wan --dport 8080 -j DNAT --to-destination 192.168.10.10:80

In Web interface



Back to NAT page, you can see a rule that you had added.

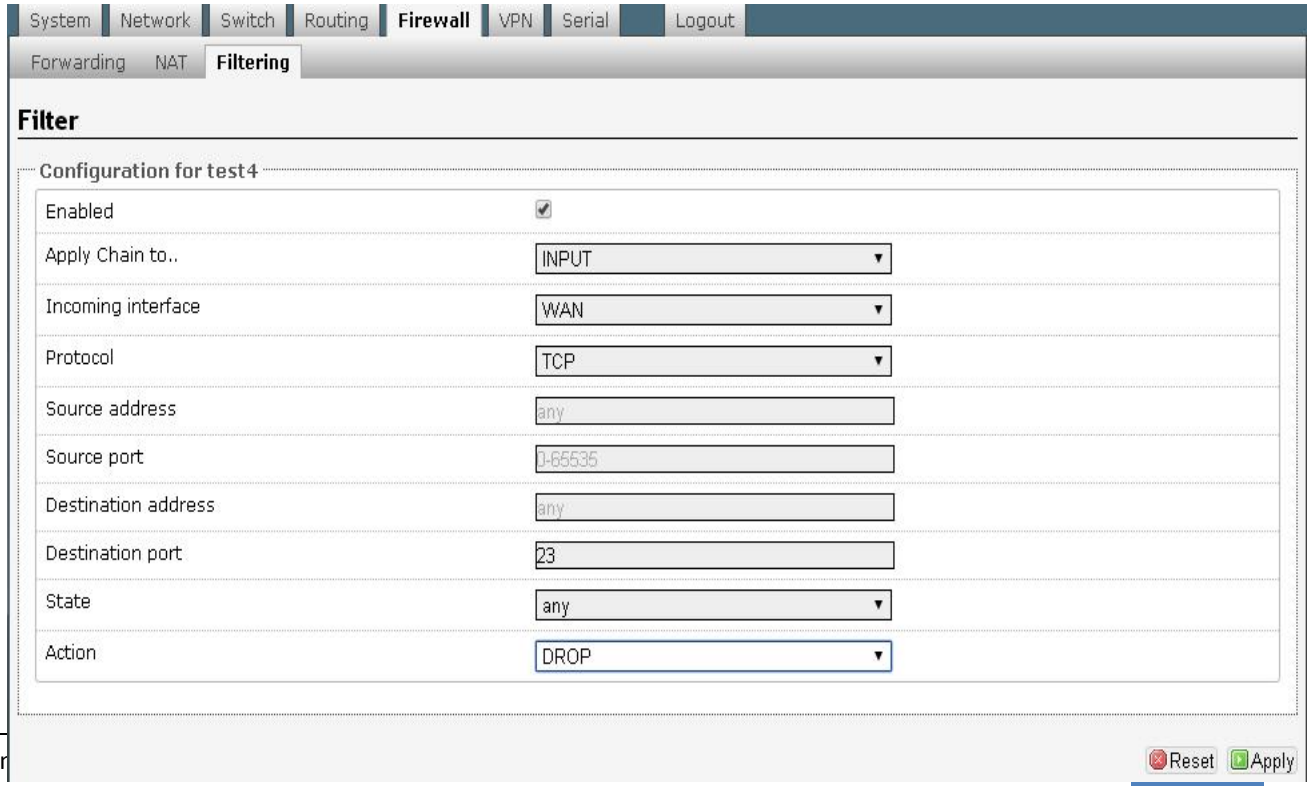


If you want to delete the rule, just click delete button and press “Apply”.

6-3 Filter

In this page, we provide INPUT and OUTPUT chain for user to specify their rules.
For example : If we do not want to access any telnet connection, we can use this command
iptables -A INPUT -i wan -p tcp --dport 23 -j DROP

In Web interface



Back to Filtering page, you can see a rule that you had added.

If you want to delete the rule, just click delete button and press “Apply”.

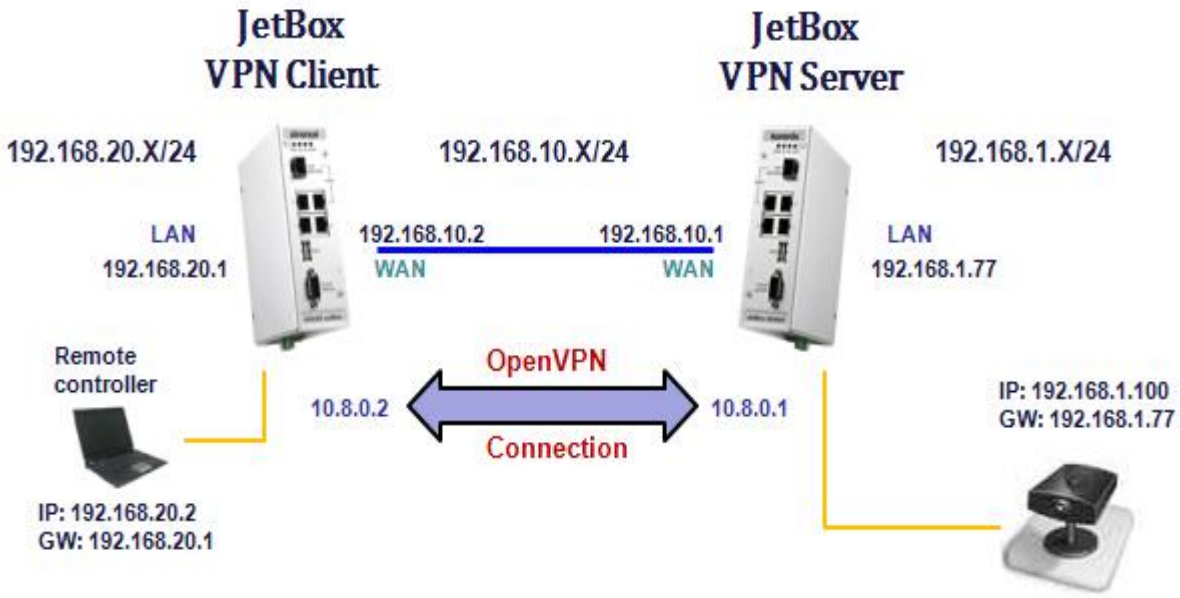
Chapter 7 VPN

In this chapter, we only provide the basic and simple configuration for user set up the various VPN connections. You can set up the VPN easily via web interface. If your environment is more complicated. We will recommend you to go into JetBox console and use command line and configuration file to set up.

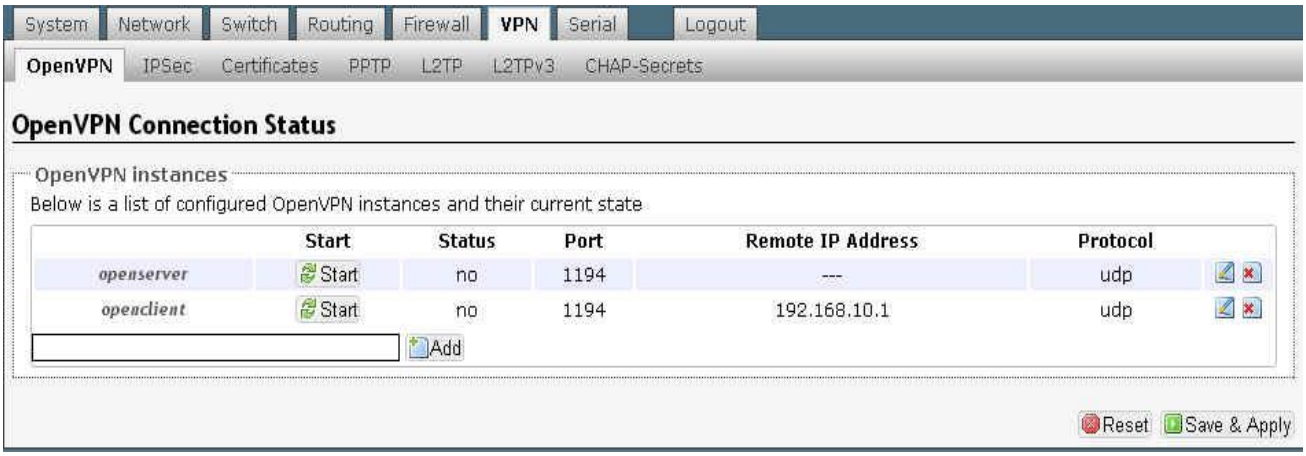
7-1 OpenVPN

Simple Example

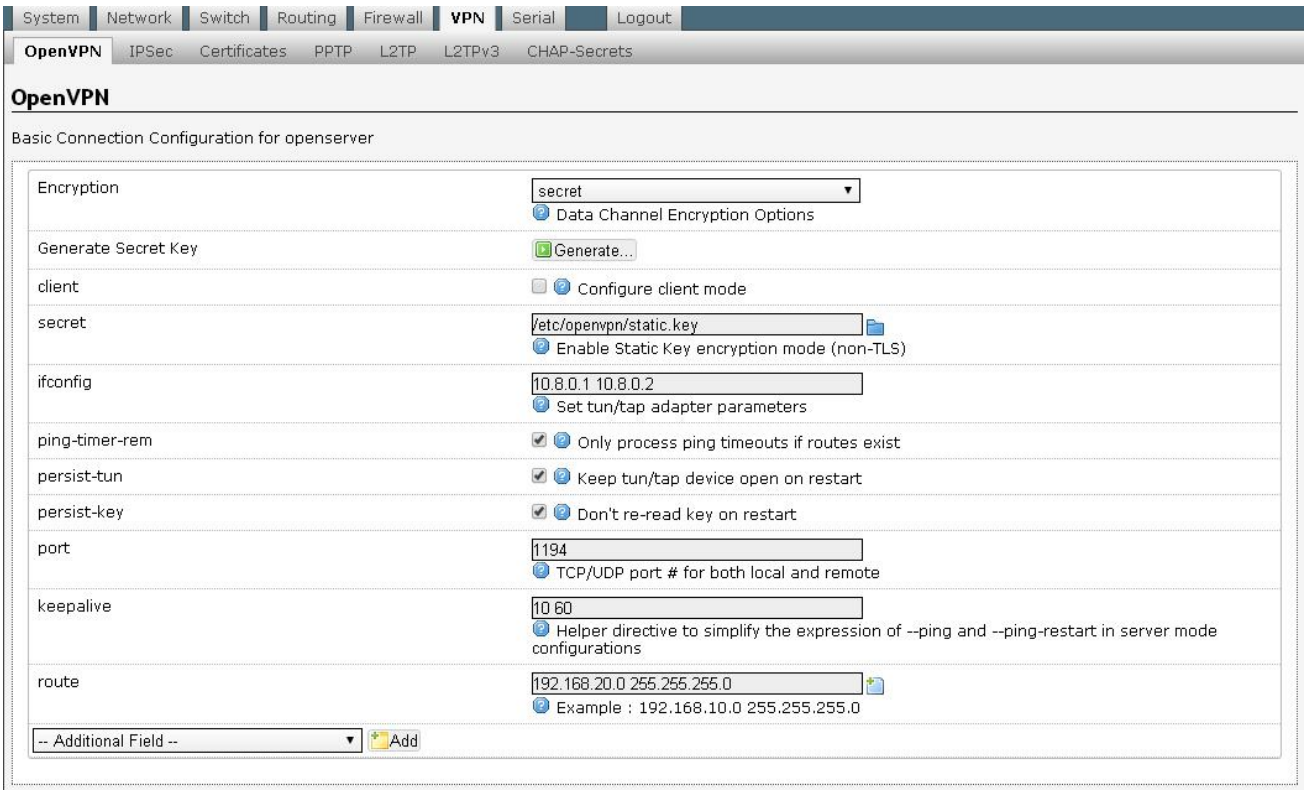
A VPN tunnel will be created with a server **vpn endpoint** of 10.8.0.1 and a client **vpn endpoint** of 10.8.0.2. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN port.



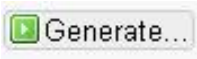
We already provide two sample configuration files for Server and Client.



Create OpenVPN Server Configuration

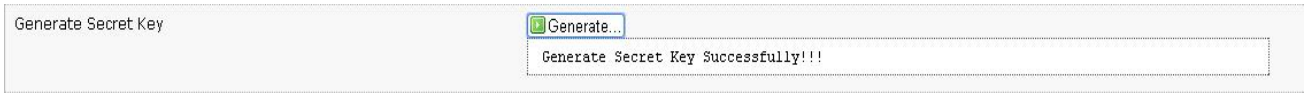


We use a pre-shared secret key **(Static Key mode)** mode.

You have to generate a static key first. You can press 

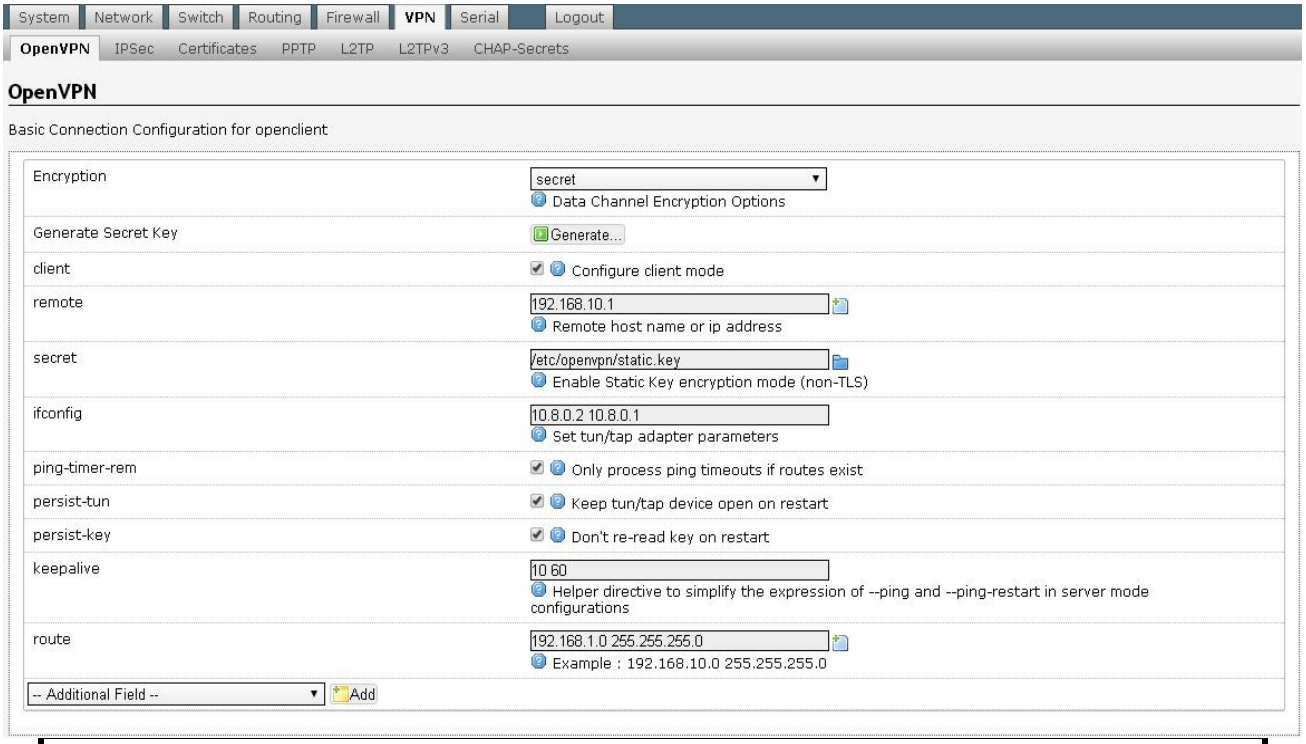
button directly with the web interface. Or type the following command In JetBox console:

```
# openvpn --genkey --secret /etc/openvpn/static.key
```



And you can select your key file. As below.

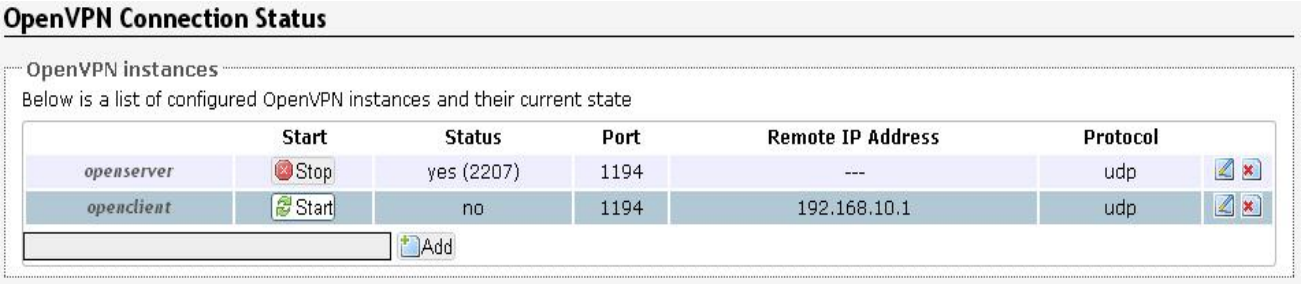
Create OpenVPN Client Configuration



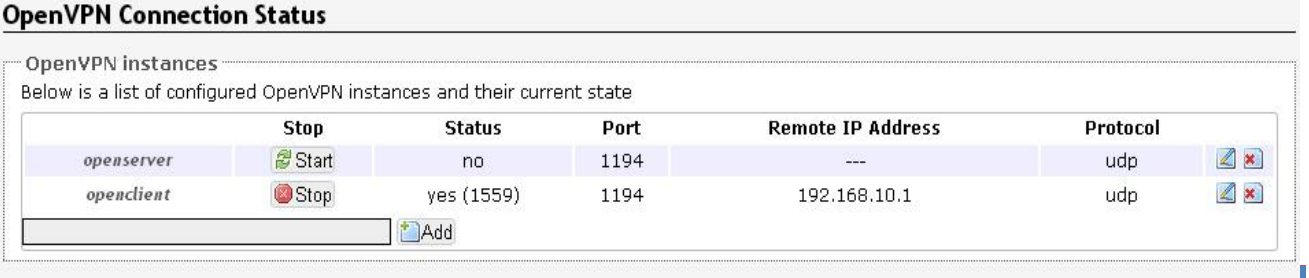
NOTE

- Static key of Client must **the same** as server. So you have to copy the static key from server. Can't generate another key on client site.

Run VPN Server in server site



Run VPN Client in client site



Test your VPN connection

For VPN client, test your VPN server is connected

```
# ping 10.8.0.1
```

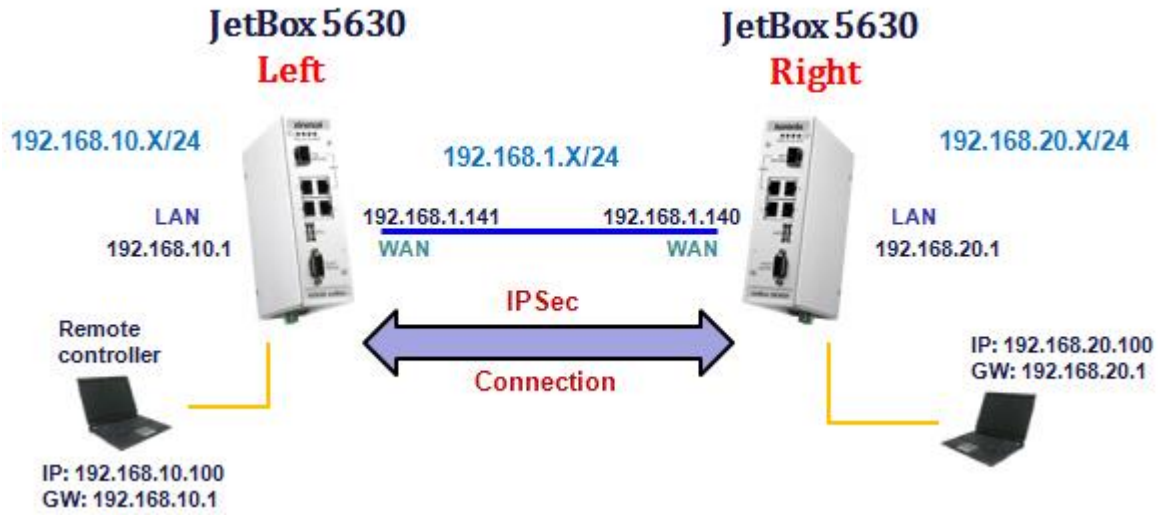
Sit at one of your local subnet nodes *(192.168.20.1)*, and ping a subnet node on the other *(192.168.1.77)*.

```
# ping 192.168.1.77
```

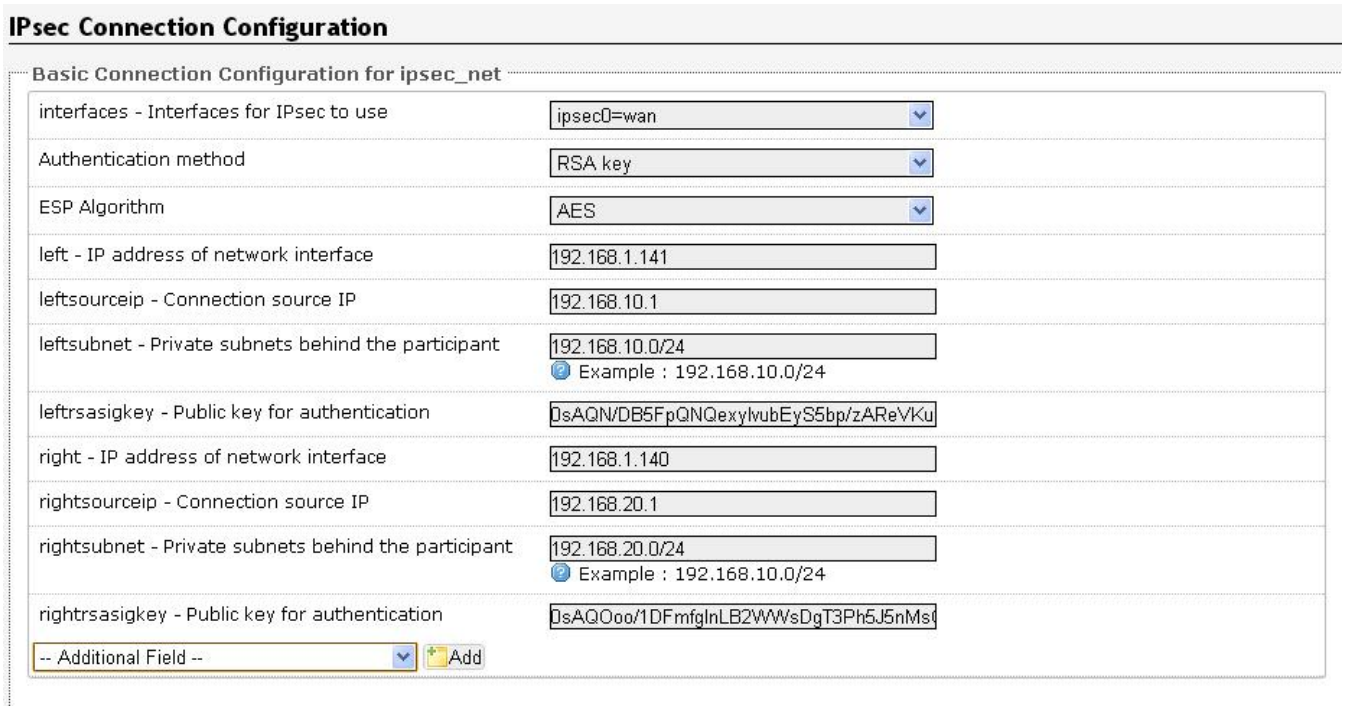
7-2 IPSec

Simple Example

The VPN tunnel has two participants on its ends, called **left** and **right**, and which participant is considered left or right is arbitrary. You can configure various parameters for these two ends via web interface.



It defines a tunnel between two nodes on the same LAN, with the left one as 192.168.1.141 and the right one as 192.168.1.140, as follows:

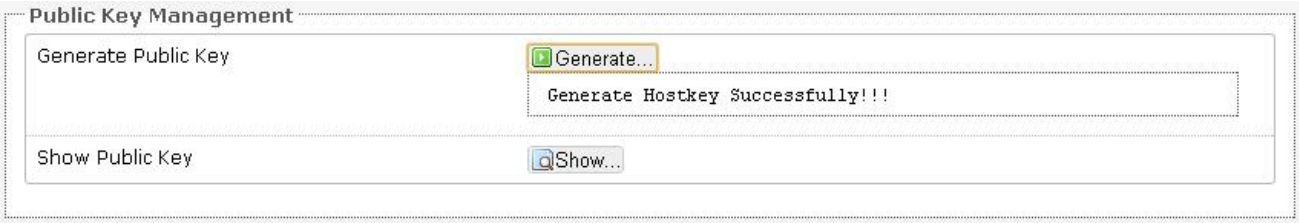


All settings are the same as /etc/ipsec.conf in JetBox 5630 console.

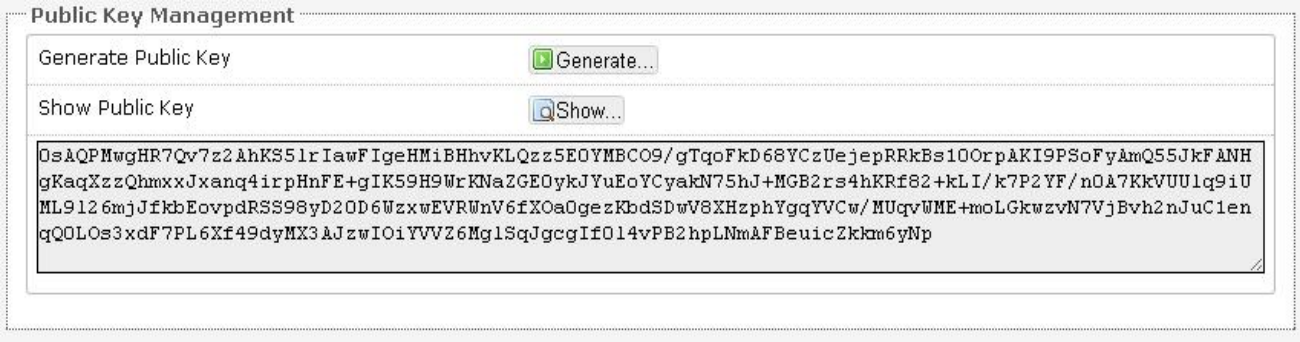
Generate a new IPsec RSA key on Left and Right

In web interface, we provide that user can generate RSA key automatically. Just press Generate... button. Ad below

Generate Hostkey Successfully



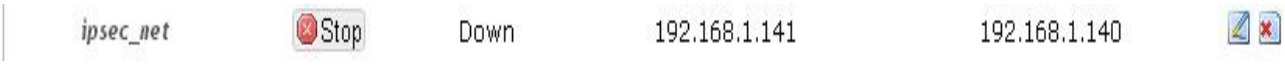
User has to fill out the leftrsasigkey/rightrsasigkey. Here you just press Show... after generate hostkey successfully. Copy it and paste to these fields.



If you are left site, you need to copy the right rsasigkey from right site. Vice versa in right site.

Start to create IPSec Tunnel

Press Start button.



Test your VPN connection

Sit at one of your local subnet nodes *(192.168.10.100)*, and ping a subnet node on the other *(192.168.20.1)*.

```
# ping 192.168.20.1
```

While still pinging, go to the right site and snoop your outgoing interface, for example:

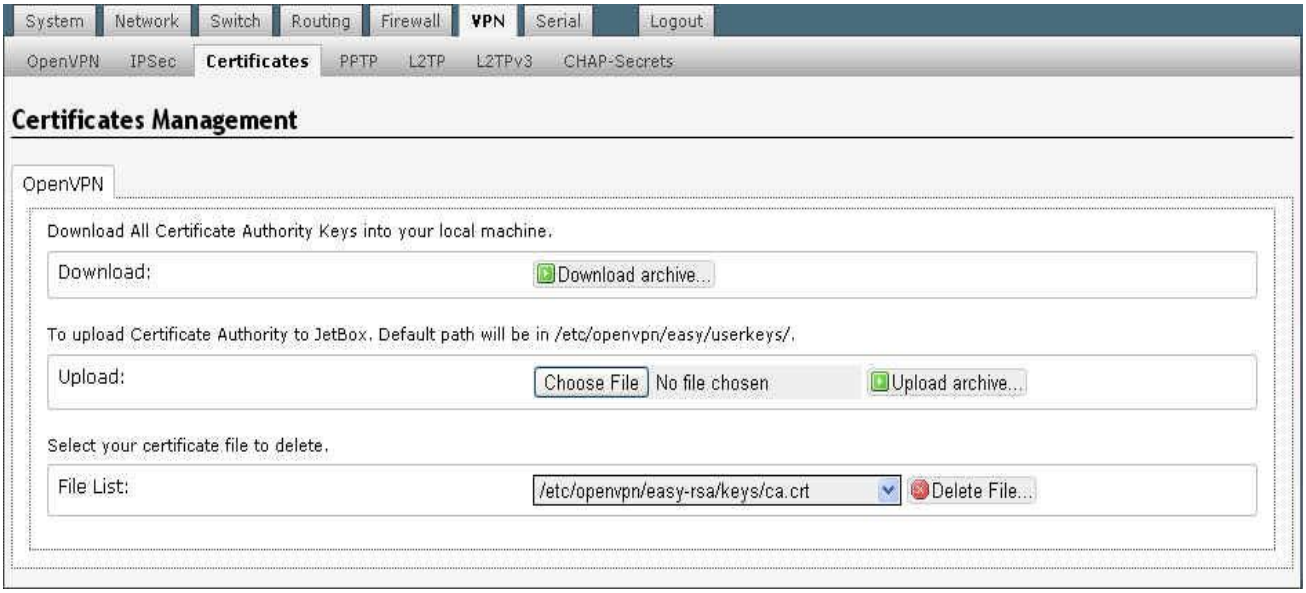
```
# tcpdump -i wan
```

You will see ESP (Encapsulating Security Payload) packets moving back and forth between the two gateways at the same frequency as your pings:

```
06:21:59.282435 IP 192.168.1.141 > 192.168.1.140: ESP(spi=0x5524c925,seq=0x17), length 100
06:22:00.282408 IP 192.168.1.141 > 192.168.1.140: ESP(spi=0x5524c925,seq=0x18), length 100
```

If you see this, congratulations are in order! You have a tunnel which will protect any IP data from one subnet to the other, as it passes between the two gates.

7-3 Certificates



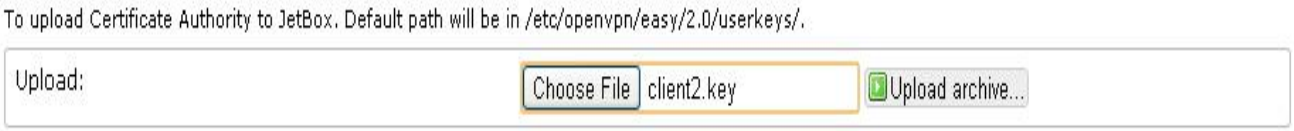
Sometimes we need to set up your own Certificate Authority (CA) and generate certificates and keys for an OpenVPN server and multiple clients. So we need to management these keys, for example, delete, backup or copy it to other clients. In this page, you can manage certificate keys of OpenVPN.

Usually, these keys are in the /etc/openvpn/easy-rsa/2.0/keys/. As below

```
/etc/openvpn/easy-rsa/2.0/keys $ ls
01.pem              client1.csr         client3.key         serial.old
02.pem              client1.key         dh1024.pem          server.crt
03.pem              client2.crt         index.txt           server.csr
04.pem              client2.csr         index.txt.attr      server.key
ca.crt              client2.key         index.txt.attr.old
ca.key              client3.crt         index.txt.old
client1.crt         client3.csr         serial
/etc/openvpn/easy-rsa/2.0/keys $
```

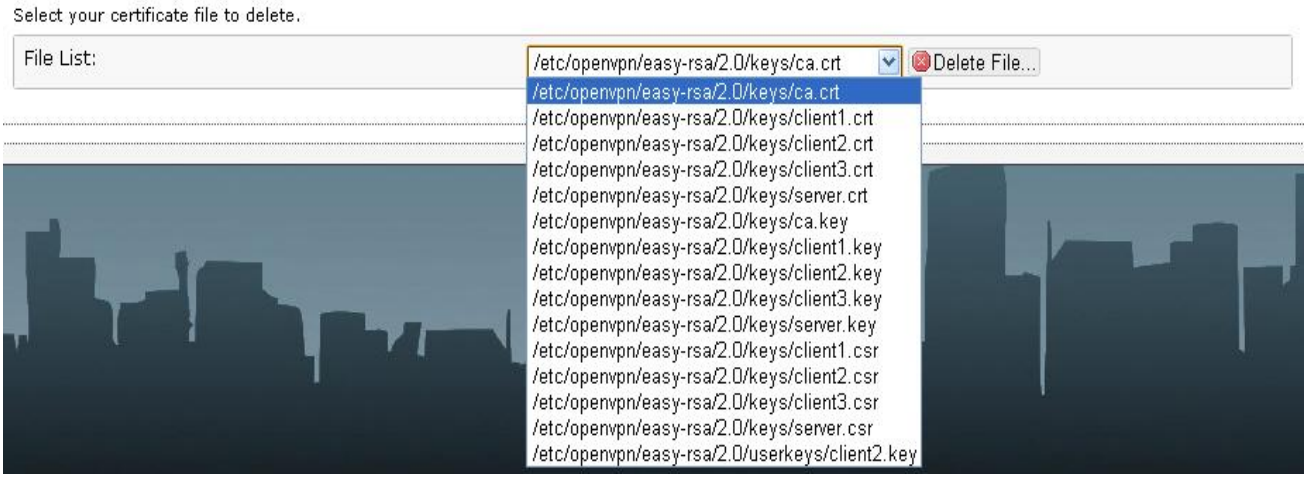
If you want to backup these keys, click Download archive... and it will compress all files in /etc/openvpn/easy-rsa/2.0/keys/ and /etc/openvpn/easy-rsa/2.0/userkeys/.

When you download these keys, you can copy them to other clients. As below



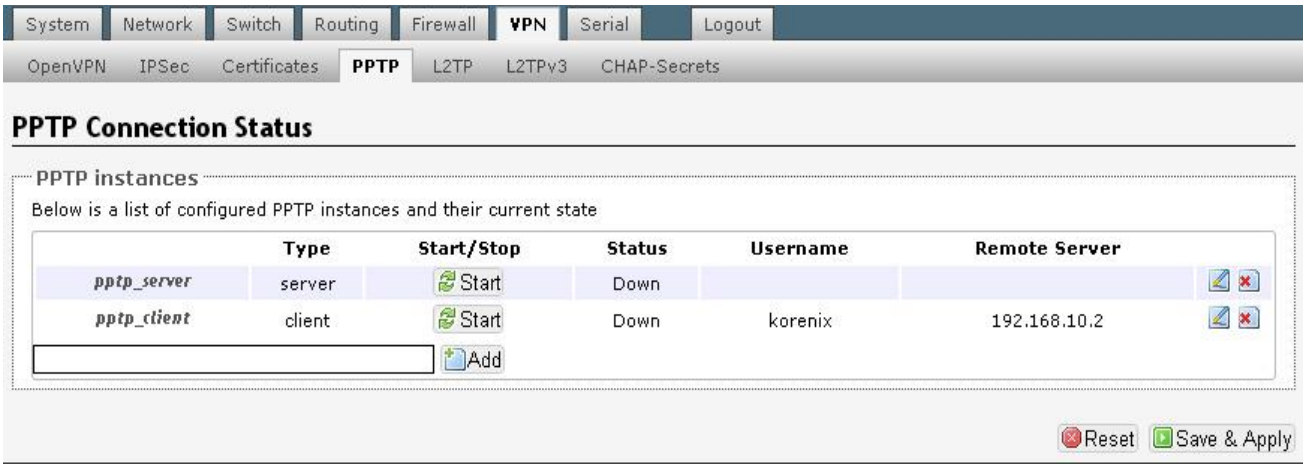
Upload path is in the **/etc/openvpn/easy-rsa/2.0/userkeys/**

You can also delete the certificate keys via web interface.



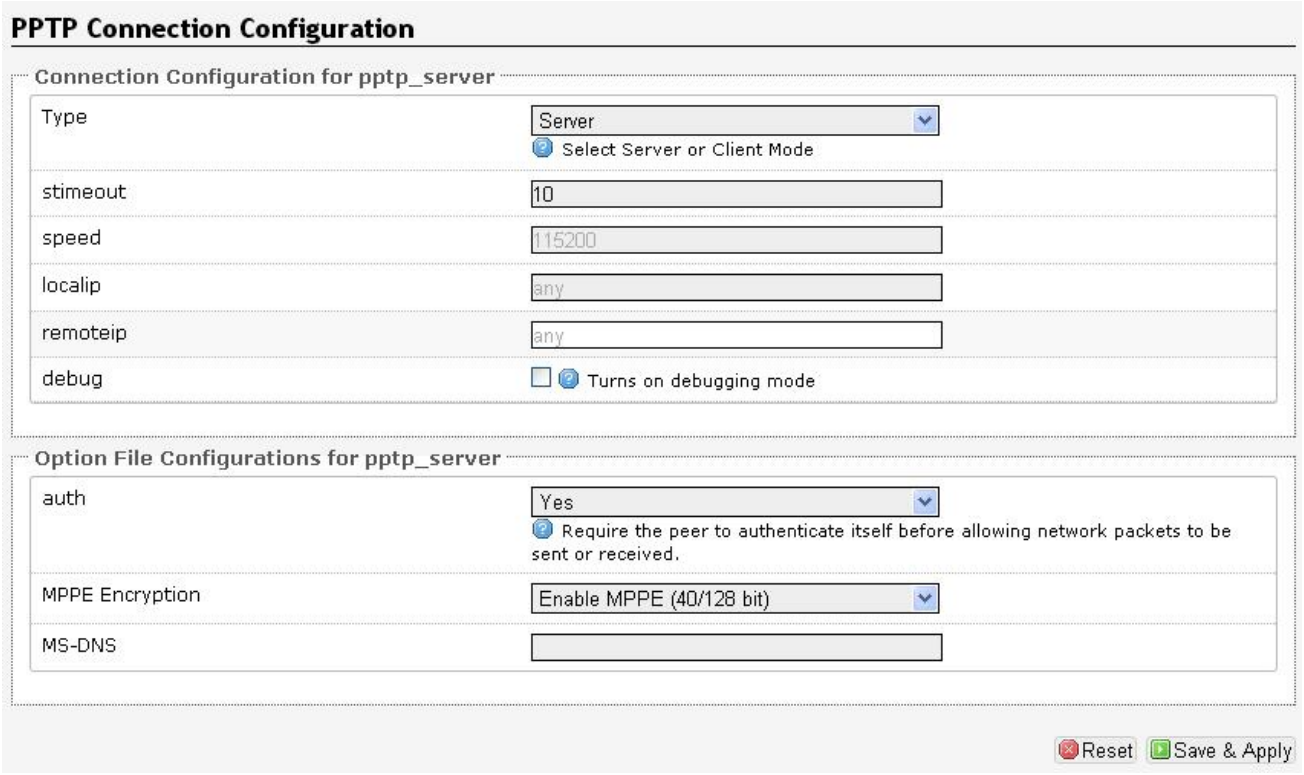
7-4 PPTP

In this page, we provide PPTP server and PPTP client for user can create a VPN tunnel based on PPTP protocol. We have two sample configurations, pptp_server, pptp_client. As below



PPTP Server Configuration

A PPTP Server (Point-To-Point Tunneling Protocol) allows you to connect securely from a remote location (such as your home) to an LAN (Local Area Network) located in another location, such as your workplace, business office, etc. This way you can use the services provided in your office at the comfort of your home.



stimeout

Number of seconds to wait for a PPTP packet before forking the **pptpctrl** program to handle the client. The default is 10 seconds.

speed

Specifies a speed (in bits per second) to pass to the PPP daemon as the interface speed for the tty/pty pair. The default is 115200 bytes per second, which some implementations interpret as meaning "no limit".

localip

One or many IP addresses to be used at the local end of the tunnelled PPP links between the server and the client. If one address only is given, this address is used for all clients. Otherwise, one address per client must be given, and if there are no free addresses then any new clients will be refused.

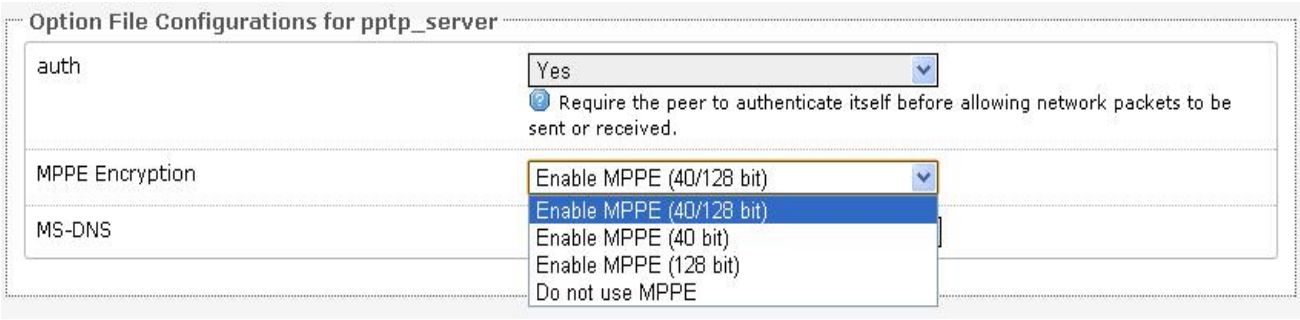
remoteip

A list of remote IP addresses to be used on the tunnelled PPP links between the server and the client.

debug

Turns on debugging mode.

Option File Configuration For PPTP Server

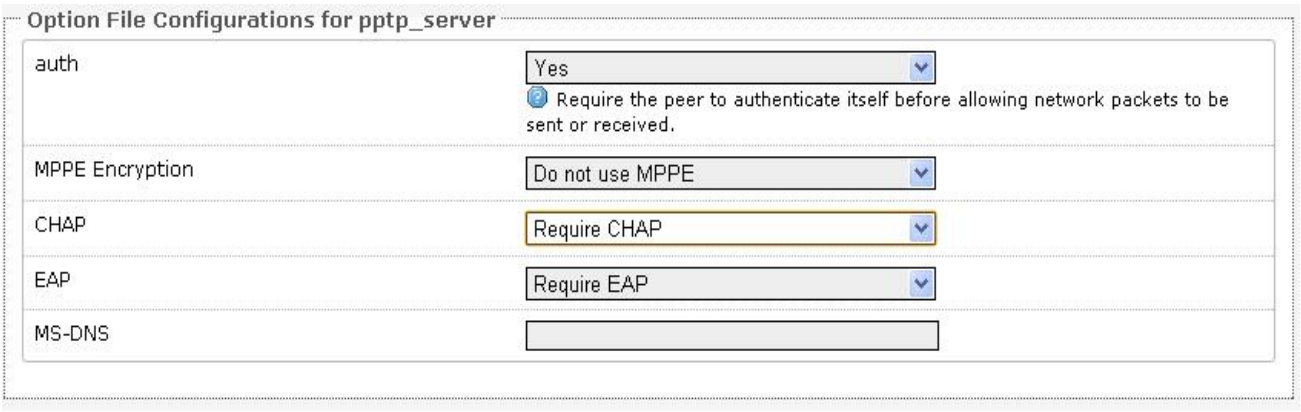

Option File Configurations for pptp_server
auth
Yes
Require the peer to authenticate itself before allowing network packets to be sent or received.
MPPE Encryption
Enable MPPE (40/128 bit)
Enable MPPE (40/128 bit)
Enable MPPE (40 bit)
Enable MPPE (128 bit)
Do not use MPPE
MS-DNS

auth

Require the peer to authenticate itself before allowing network packets to be sent or received.

MPPE Encryption

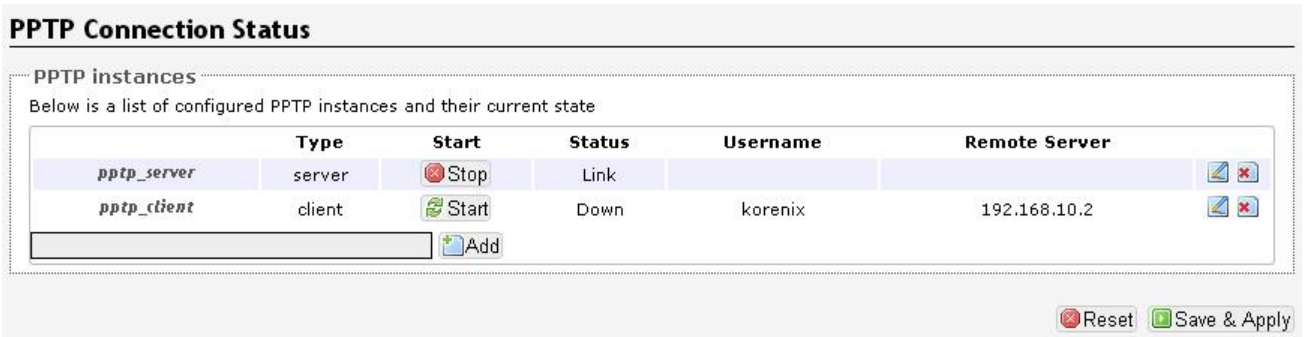
Here we provide three MPPE encryption types, MPPE with 40/128-bit, MPPE with 40-bit, MPPE with 128-bit. If you want to use CHAP or EAP encryption, select “Do not use MPPE” and you will see these options.



MS-DNS

If pppd is acting as a server for Microsoft Windows clients, this option allows pppd to supply one or two DNS (Domain Name Server) addresses to the clients.

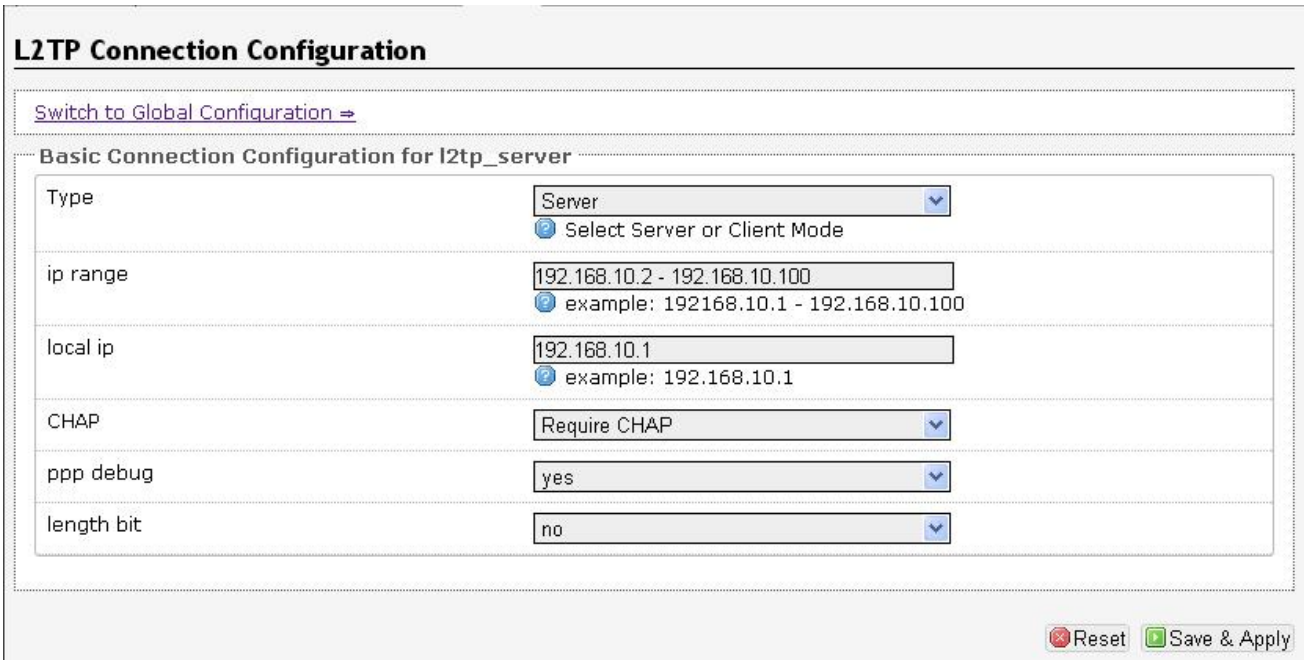
Click “**Save&Apply**” and back to PPTP pages. Press button to start PPTP server and Client.



7-5 L2TP

Here we provide the basic L2TP settings. User can create L2TP tunnel easily via web interface. There are two sample configurations, l2tp_server, l2tp_client.

L2TP Server Configuration



ip range

Specify the range of ip addresses the LNS will assign to the connecting LAC PPP tunnels. Multiple ranges can be defined. Ranges are defined using the format IP - IP (example: 1.1.1.1 - 1.1.1.10).

local ip

Use the following IP as xl2tpd's own ip address.

CAHP (refuse | require chap)

require or refuse the remote peer to get authenticated via CHAP for the ppp authentication.

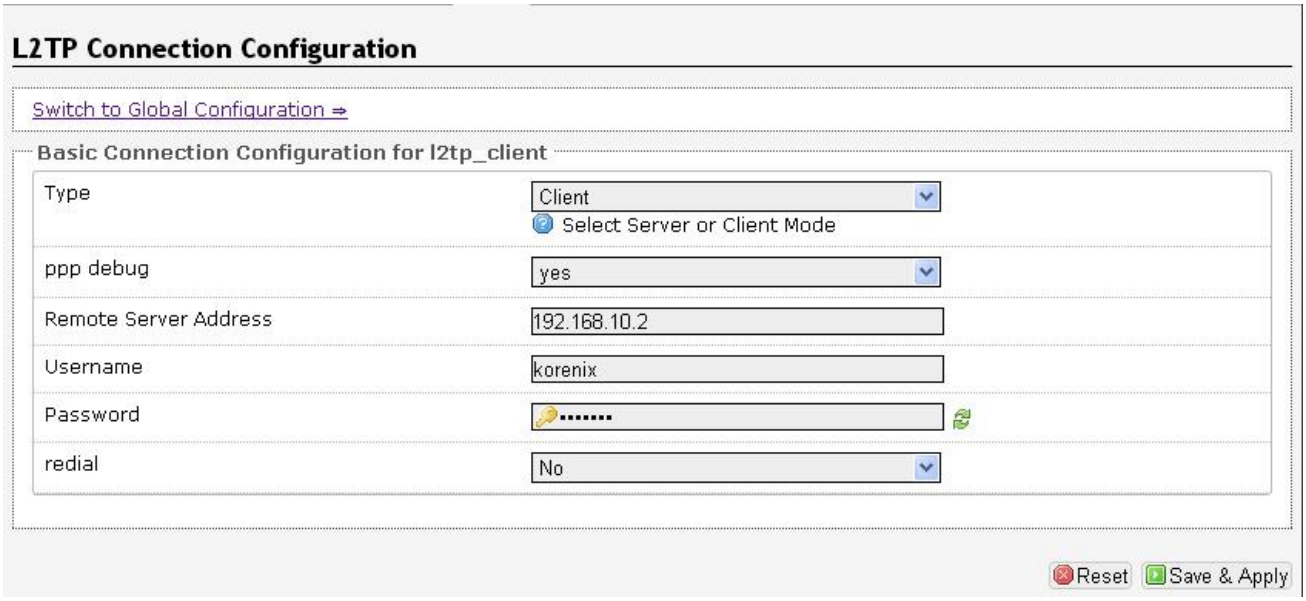
ppp debug

This will enable the debug for pppd

length bit

If set to yes, the length bit present in the l2tp packet payload will be used.

L2TP Client Configuration



Remote Server Address

Set the DNS name or IP address of the LNS to connect to.

Username

Set the name of the local system for authentication purposes to *name*.

Password

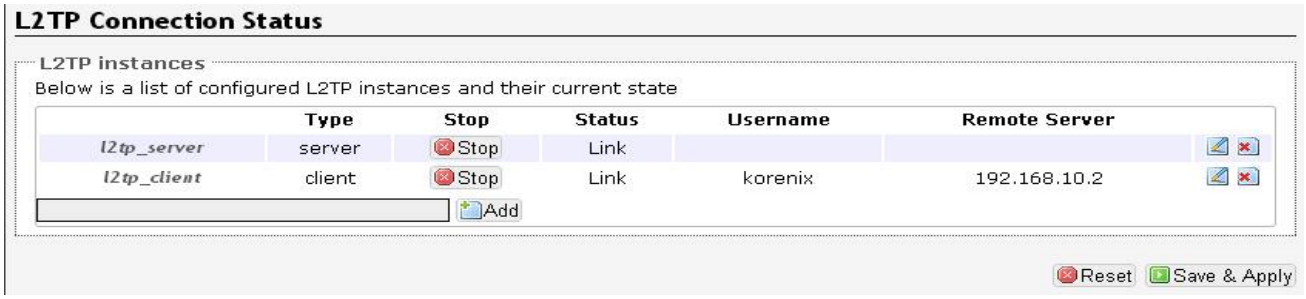
Specifies the password to use for authenticating to the peer.

redial

If set to yes, xl2tpd will attempts to redial if the call get disconected.

Remember to Press "**Save & Apply**" to apply these setting and generate configuration file.

Back to L2TP pages. Press Start button to start L2TP server and Client.

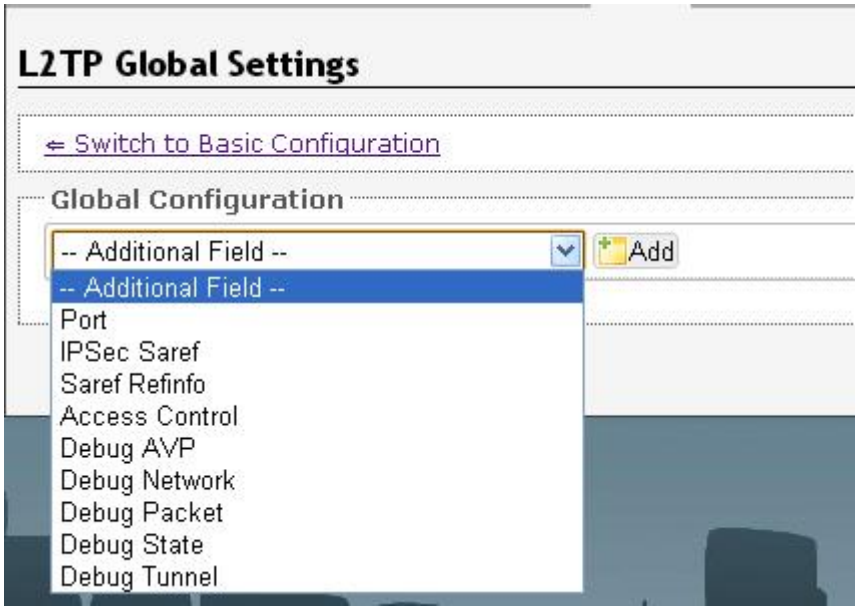


NOTE

- When you press start button with l2tp_client, it will also start l2tp_server. It is normally. So remember to stop l2tp_server if you do not want to enable l2tp daemon anymore.

Switch to Global Configuration

We also provide the Global section for L2TP. As below



port

Specify which UDP port xl2tpd should use. The default is 1701.

ipsec saref

Use IPsec Security Association trackinng. When this is enabled, packets received by xl2tpd should have to extra fields (refme and refhim) which allows tracking of multiple clients using the same internal NATed IP address, and allows tracking of multiple clients behind the same NAT router. Values can be yes or no. The default is no.

saref refinfo

When using IPsec Security Association trackinng, a new setsockopt is used. If not set, the default is to use 30.

access control

If set to yes, the xl2tpd process will only accept connections from peers addresses specified in the following sections. The default is no.

debug avp

Set this to yes to enable syslog output of L2TP AVP debugging information.

debug network

Set this to yes to enable syslog output of network debugging information.

debug packet

Set this to yes to enable printing of L2TP packet debugging information. Note: Output goes to STDOUT, so use this only in conjunction with the **-D** command line option.

debug state

Set this to yes to enable syslog output of FSM debugging information.

debug tunnel

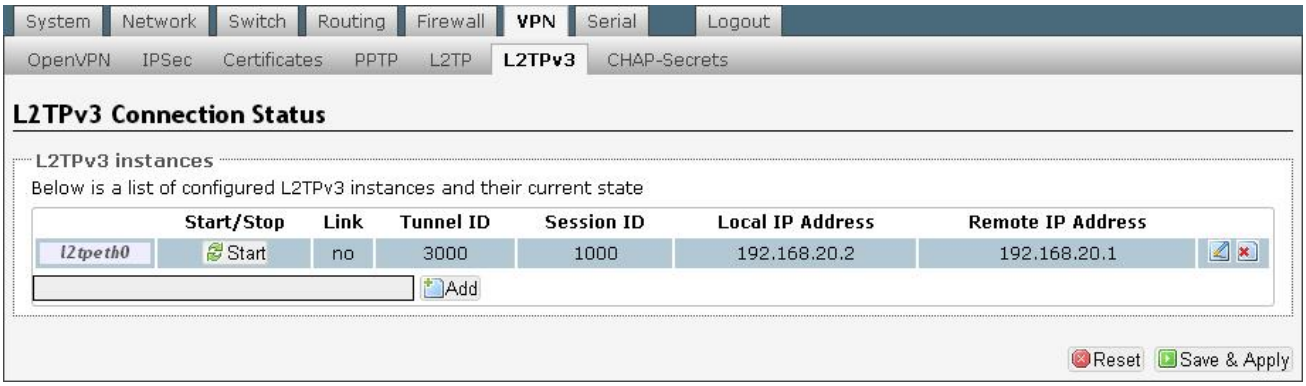
Set this to yes to enable syslog output of tunnel debugging information.

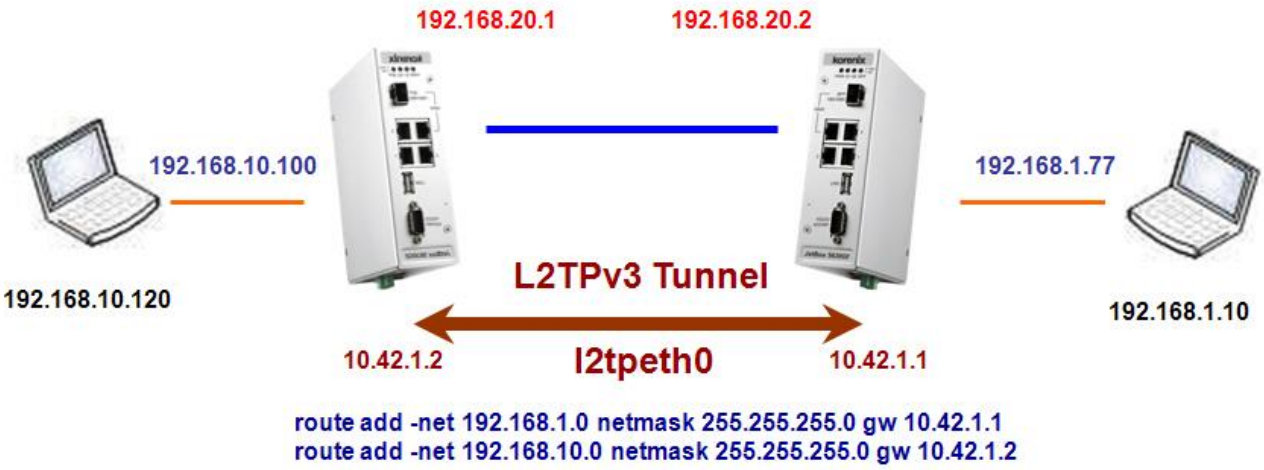
Basically, you can create L2TP tunnel easily by using basic configuration.

7-6 L2TPv3

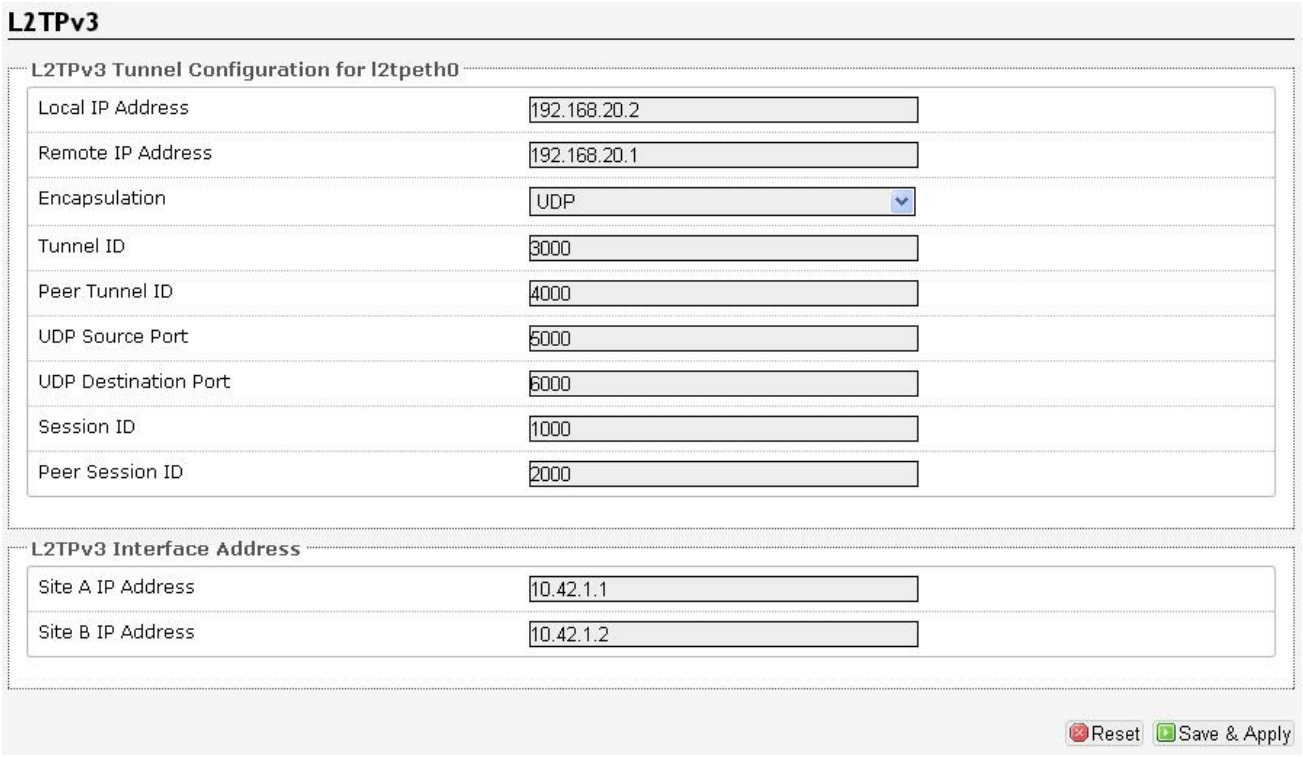
In web interface, we provide L2TPv3 section for user can create L2TPv3 tunnel easily.

There is a sample configuration as below.





L2TPv3 Configuration



All the settings are the same as command in JetBox 5630 console.

For example

Site A : 10.42.1.1

```
~$ /sbin/ip l2tp add tunnel tunnel_id 3000 peer_tunnel_id 4000 encap udp local
192.168.20.1 remote 192.168.20.2 udp_sport 5000 udp_dport 6000
```

```
~$ /sbin/ip l2tp add session tunnel_id 3000 session_id 1000 peer_session_id 2000
```

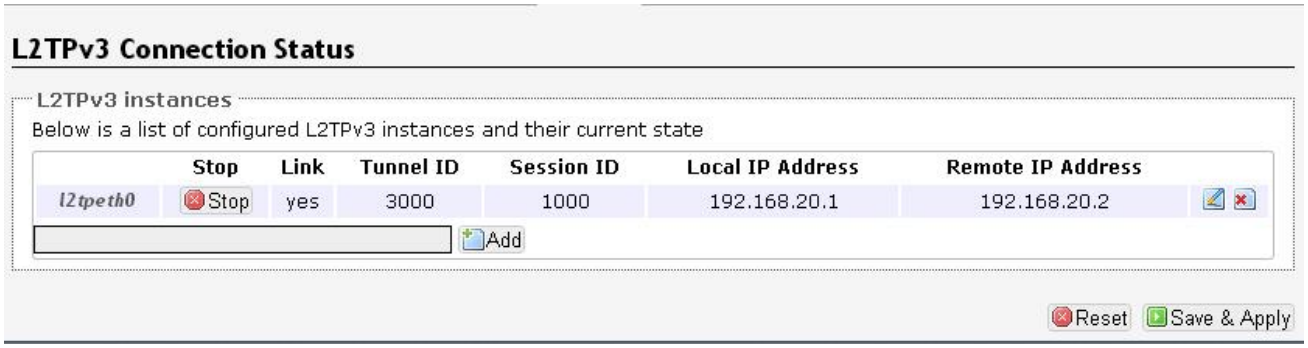
```
~$ /sbin/ip link set l2tpeth0 up
```

```
~$ /sbin/ip addr add 10.42.1.1 peer 10.42.1.2 dev l2tpeth0
```

Some important parameters, like **tunnel_id, peer_tunnel_id, udp_sport, udp_dport …etc.** You have to specify as same as ip command in JetBox 5630 console.

Press "**Save&Apply**" and back to L2TPv3 page. Press

to create L2TPv3 tunnel.



7-7 CHAP-Secrets

If you are using chap authentication, then you also need to create the secrets file. It is /etc/ppp/pap-secrets

The CHAP secrets file

The current pppd version requires that you have mutual authentication methods - that is you must allow for both your machine to authenticate the remote server **AND** the remote server to authenticate your machine.

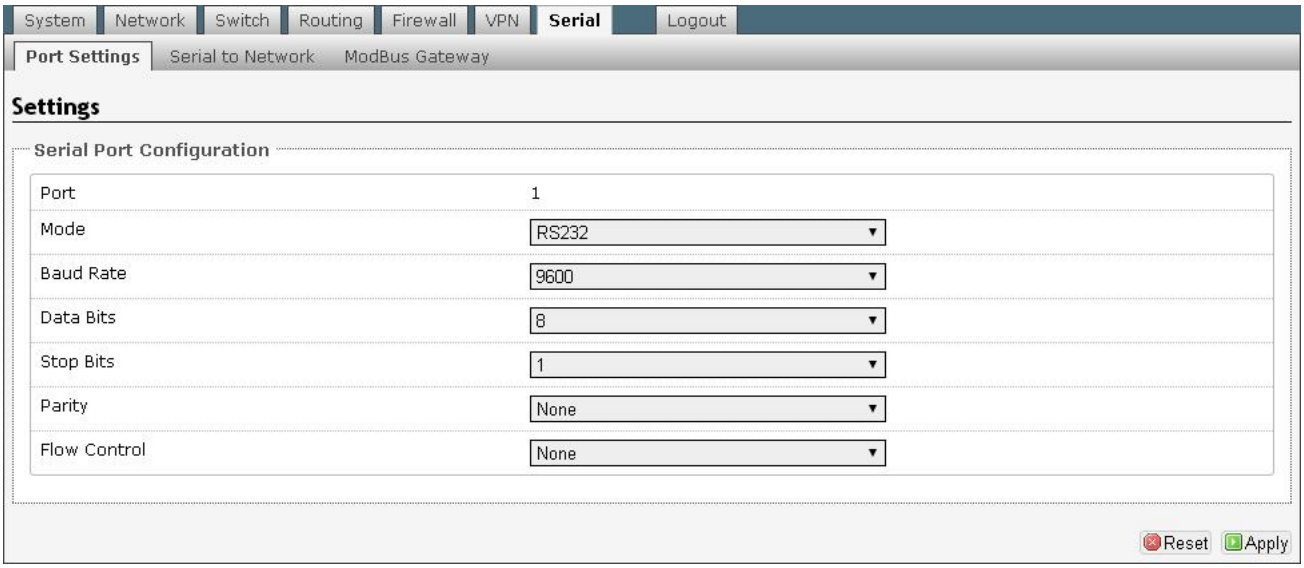
The field can be a symbol “*”. It means any username or hostname.

Chapter 8 Serial

In this chapter, we will explain how to set up the mode of serial port via web interface.

8-1 Port Settings

In this page, user can set up the mode of serial port. As below



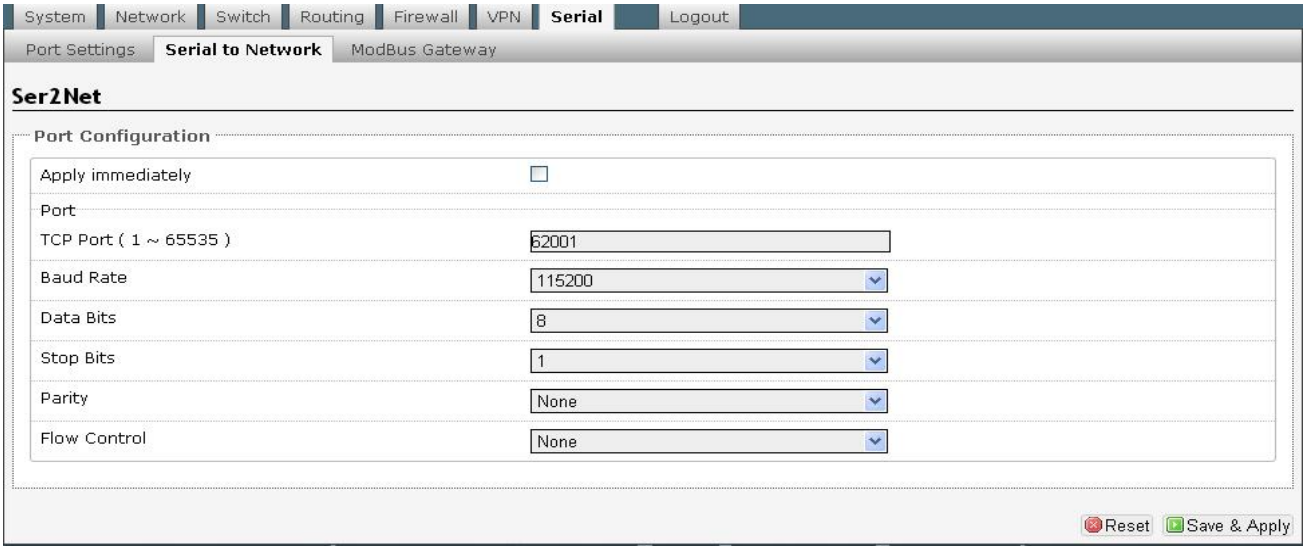
Mode

We provide RS232、RS422、RS485 4 Wire for user select. It is the same as **serialctl** command.

The other parameters are the same as general settings of serial port.

8-2 Serial to Network

In this page, user can set up the ser2net function. As below

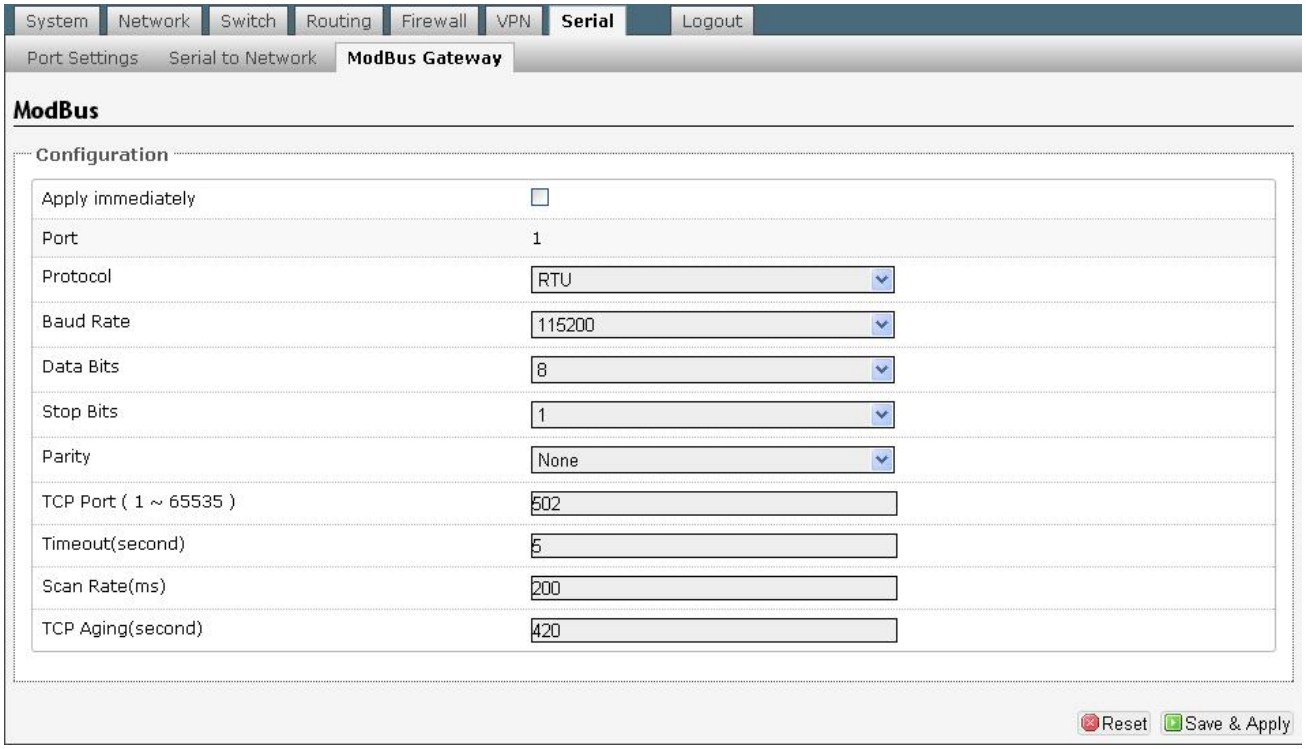


Apply immediately

It means that start **ser2net** immediately. If you do not check it, it will kill all ser2net process after pressing **Save&Apply** button.

8-3 ModBus Gateway

In this page, we provide the modbus gateway for user can set up. If you don't have modbus gateway program, it will not run.



Apply immediately

It means that start **modbus** immediately. If you do not check it, it will kill all modbus process after pressing **Save&Apply** button.

Protocol

Set Modbus protocol. **Default : RTU**

Baud Rate

Set data transfer rate. **Default: 115200**

Data Bits

Set the length of each data. **Default: 8 bits**

Stop Bits

Set the length of stop bit. **Default: 1**

Parity

Set parity check parameters to avoid errors during data transferring. **Default: None**

TCP Port

Set the port numbers of Modbus TCP server from 1~65535. **Default: 502**

Timeout

Set the wait-for-respond-time of data transferring from Modbus TCP to Modbus RTU/ASCII through Modbus Gateway. Range from 0~600 seconds. **Default: 5 seconds**

Scan Rate

Set the scan rate from 0~10000ms. **Default: 200ms**

TCP Aging

The system will automatically interrupt the connection to avoid occupying channel if the TCP connection is failed or idling abnormally. Range from 1~7200 seconds. **Default: 420s**

Korenix Technology Co., Ltd.

Business service: sales@korenixembedded.com, sales@korenix.com

Customer service: koreCARE@korenix.com

Web Site: http://www.korenixembedded.com, http://www.korenix.com